all rights reversed

HACKER

τεύχος 035 - The New Outpost Edition

Αύγουστος 2014 # Τιμή τεύχους 4€

Αποκαλυπτικό port scanning, με το ικανότατο nmap [*]

Τα πανίσχυρα NSE scripts

Ρυθμίστε το OpenVPN στο pfSense

Βγάλτε βόλτα την Python [μέρος 2]

Hacking με το Android smartphone σας

[*] Αφιέρωμα για αρχάριους αλλά και για πιο προχωρημένους ;)

all rights reversed

HACKER

Περιεχόμενα

και οδηγίες χρήσης

52

Το nmap πέρα από τα βασικά

Εξετάζουμε ορισμένες πιο προχωρημένες δυνατότητες του nmap και παίζουμε με την πανίσχυρη scripting engine του προγράμματος

68

Βάλτε τη δική σας σφραγίδα στο Android

Καταστήστε την οθόνη έναρξης της συσκευής μοναδική κι απόλυτα προσωποποιημένη

76

Βγάλτε βόλτα την Python [μέρος 2]

Μάθετε πώς να παράγετε αυτοτελή εκτελέσιμα αρχεία, ώστε τα προγράμματά σας να διακινούνται με ακόμα μεγαλύτερη ευκολία!

online

Το OpenVPN στο pfSense

http://deltahacker.gr/openvpn-pfsense

Εκδότης / Διευθυντής	Χρήστος Βαρελάς
Αρχισυντάκτης	Παναγιώτης Βαρελάς
Σύμβουλοι έκδοσης	Νίκος Μουρατίδης, Βούλα Παυλίδου
Σύνταξη	Γιώργος Αραβίδης, Παναγιώτης Βαρελάς, Χρήστος Βαρελάς, Ανδρέας Βενιέρης, Γιώργος Γιάννου, Μανώλης Κιαγιάς, Ιωάννης Κονιάρης, Πέτρος Κυλαδίτης, Γιώργος Μελέκος, Νίκος Μουρατίδης, Θωμάς Σερμπίνης, Νικόλαος Σηφάκης, Μέσος Παπαδόπουλος (TM), Χρίστος Τόμπρας
Γραμματική επιμέλεια	Βούλα Παυλίδου
Καλλιτεχνική Επιμέλεια	Πέτρος Φιλιππίδης

Το ηλεκτρονικό περιοδικό deltaHacker είναι συνδρομητικό και εκδίδεται από την Parabing Creations δώδεκα φορές το χρόνο, κάθε μήνα. Η Parabing Creations έχει την έδρα της στη Μαιώτιδος 3, 55133, Καλαμαριά. Ο δικτυακός τόπος του περιοδικού είναι στο http://deltahacker.gr. Το email επικοινωνίας είναι το talk2us@deltahacker.gr και ειδικά για τις συνδρομές είναι το subscriptions@deltahacker.gr. Οι γενικές πληροφορίες για τις συνδρομές παρατίθενται στο http://deltahacker.gr/subscriptions και οι ίδιες οι παραγγελίες γίνονται από το http://deltahacker.gr/pdf12order. Όλες οι απόψεις που εκφράζονται στα άρθρα δεν εκφράζουν απαραίτητα και τη γνώμη του περιοδικού.

greenqloud

www.greenqloud.com

Power your startup with clean energy

Join GreenQloud's Truly Green™ startup program and take advantage of:

- Free Compute Qloud™ and Storage Qloud™ usage for six months
- Access to our revered 24/7 "all hands on deck" customer support
- Highly scalable, easy-to-use cloud services at your fingertips, in seconds
- Features in GreenQloud's marketing communications
- Mentorship for you and your team with our executive team in any of the following areas: cloud architecture; software engineering or software development; business model design; marketing; sales and product strategies; and human resources
- Become part of our global startup community now!

Apply now!

greenqloud

For more information, please visit www.greenqloud.com/startup-program

Ισλαμικό Κράτος του Ιράκ και του Λεβάντε ...και Μαχητές της Ελευθερίας

by sp1ral ev0lut10n

Επιτέλους, λίγη δροσιά! Να και μια πραγματικά καλή είδηση. Δεν λέω, έχει και το καλοκαίρι τις χάρες του· κάνουμε τις βουτιές μας, πίνουμε το καφεδάκι μας δίπλα στη θάλασσα, κατεβάζουμε παγωμένες μπύρες κι όταν μερακλώνουμε, ε, ξεπαστρεύουμε τη θαλάσσια πανίδα, συνοδεία ούζου ή και άλλων αποσταγμάτων. Όλα αυτά όμως ισχύουν υπό μια προϋπόθεση: Το να μπορείς να τα απολαύσεις. Δεν ξέρω αν φέτος ήταν περισσότεροι ή λιγότεροι εκείνοι που εξόρμησαν στις παραλίες, αλλά μπορώ να σας πω με βεβαιότητα ότι υπήρξαν πολλοί, μα πάρα πολλοί, που παρέμειναν στα σπίτια τους. Όχι από επιλογή τους, φυσικά.

Όπως και να 'χει, τώρα που το θερμόμετρο αποφάσισε να κατηφορίσει δεν υπάρχει κανένας που να μην ανακουφίζεται. Από τη μία, όσοι κατάφεραν να πάνε διακοπές χαίρονται, γιατί το περιβάλλον στο οποίο επέστρεψαν έπαψε να τους θυμίζει τις διακοπές που τελείωσαν. Από την άλλη, χαίρονται κι εκείνοι που δεν πήγαν πουθενά, γιατί ο καιρός έπαψε να τους υπενθυμίζει αυτά που στερήθηκαν.

Θα σκεφτεί κανείς ότι μιλάω για τη δροσιά, λες και το μεγαλύτερο πρόβλημα που αντιμετωπίζει ο κόσμος είναι η υπερβολική ζέστη κι όχι, ας πούμε, τα τεράστια ποσοστά ανεργίας και η αυξημένη φορολογία, σε συνδυασμό με την κατακρήμνιση μισθών και εργασιακών δικαιωμάτων. Μην ανησυχείτε για την ισορροπία μου! Γνωρίζω πολύ καλά ότι η πρόσφατη πτώση της θερμοκρασίας επέφερε μια πρόσκαιρη και σίγουρα πολύ μικρή ανακούφιση.

Ας επιστρέψομε όμως στις ειδήσεις: Τα καλά νέα είναι ότι δρόσισε! Κι επιμένω όχι μόνο γιατί είχα πλαντάξει από τη ζέστη, αλλά κυρίως γιατί αποτελεί ένα αδιαμφισβήτητο γεγονός. Η περιγραφή του είναι σύντομη, απλή, ξεκάθαρη και δεν κρύβει καμία δόλια πρόθεση. Το ακριβώς αντίθετο, δηλαδή, σε σχέση με όσα λέγονται στα δελτία ειδήσεων.

Οι Τζιχαντιστές είναι κακοί... πολύ κακοί! Μιλάω ειρωνικά, αλλά μη νομίζετε ότι διαφωνώ με την πρόταση αυτή καθ' αυτή. Θα μπορούσα να αποδώσω και βαρύτερους χαρακτηρισμούς στους Τζιχαντιστές, όπως εγκληματίες, αποβράσματα και πάει λέγοντας. Το αντικείμενο της ειρωνείας μου είναι η δήθεν δίψα των ΜΜΕ για "αμερόληπτη" και "αντικειμενική" ενημέρωση. Το πρόβλημά μου δεν έχει να κάνει με την άποψη που διατηρώ για τους Τζιχαντιστές. Η παραπάνω πρόταση, αν και διατυπωμένη με ύφος ελαφρύ και σχεδόν αστείο, με βρίσκει απόλυτα σύμφωνο. Αυτό που με ενοχλεί είναι οι προτάσεις που *δεν* λέγονται.

Η μανία των ΜΜΕ για άμεση και έγκυρη ενημέρωση είναι απερίγραπτη. Τα ειδησεογραφικά τους επιτελεία εργάζονται ακούραστα. Δίνουν τη μάχη της ενημέρωσης νύχτα–μέρα και δεν λυγίζουν μπροστά σε τίποτα. Το τελευταίο διάστημα, για παράδειγμα, όσο σκληρή κι αν είναι η πραγματικότητα, σφίγγουν το στομάχι τους και περιγράφουν κάθε εγκληματική πράξη και κάθε προκλητική ενέργεια των Τζιχαντιστών. Βέβαια, τι να σου κάνουν και τα στελέχη των ειδησεογραφικών επιτελείων...Άνθρωποι είναι και κουράζονται και καμιά φορά ξεχνούν...

Ας θυμηθούμε λοιπόν, μαζί. Το 1979 Αμερικανοί και Βρετανοί χρηματοδοτούσαν διάφορες ισλαμιστικές ομάδες, ενώ εργάζονταν και για τη δημιουργία νέων, με στόχο το χτύπημα του Αφγανιστάν. Από αυτά τα φυτώρια προέκυψε ο γνωστός Οσάμα Μπιν Λάντεν, όπως επίσης οι Ταλιμπάν και η οργάνωση Αλ-Κάιντα, που είχε στενές σχέσεις με τη CIA. Κι όλα αυτά δεν αποτελούν θεωρίες συνωμοσίας. Πρόκειται για γεγονότα που παραδέχτηκε και ο πρόεδρος των ΗΠΑ Τζ. Μπους (ο πατήρ).

Από τότε έγιναν αρκετοί πόλεμοι στην περιοχή, πάντα με πρόσχημα την "αντιμετώπιση της τρομοκρατίας" και την "υπεράσπιση των ανθρωπίνων δικαιωμάτων". Για μια στιγμή, όμως, γιατί στο τέλος θα ξεχάσουμε κι αυτά που ξέρουμε! Υπάρχει σκεπτόμενος άνθρωπος που να πιστεύει ότι αυτοί οι πόλεμοι έγιναν για την ευημερία του απλού κοσμάκη; Φυσικά κι όχι. Στόχος ήταν η κλοπή των ενεργειακών πόρων και ο έλεγχος των δρόμων μεταφοράς τους. Ακριβώς γι' αυτό, η τακτική που ακολουθούσαν οι "μαχητές της Ελευθερίας" ήταν αυτή του διαίρει και βασίλευε. Κάπως έτσι ξεπηδούσαν διάφορες ένοπλες ισλαμιστικές οργανώσεις, όπως είναι και το "Μέτωπο Αλ Νούσρα", που εξαπολύθηκε εναντίον της Συρίας. Ε, λοιπόν, από

όλες αυτές τις οργανώσεις προέκυψε και το "Ισλαμικό Κράτος του Ιράκ και του Λεβάντε", που αργότερα μετονομάστηκε σε "Ισλαμικό Κράτος" (Σ.τ.Ε. Για λόγους μάρκετινγκ, καταλαβαίνετε.) Σας θυμίζει κάτι αυτό; Σήμερα αποκαλούνται "Τζιχαντιστές του Ισλαμικού Κράτους".

Ενδιαφέροντα στοιχεία που είτε παραλείπονται από τα δελτία ειδήσεων είτε περνούν στα ψιλά, υπάρχουν και στο πρόσφατο παρελθόν. Για παράδειγμα, λίγο μετά τον πόλεμο στη Λιβύη αποκαλύφθηκε ότι ο "αγανακτισμένος λαός", οι επαναστάτες που είχαν ξεσηκωθεί εναντίον του Καντάφι, είχαν εξοπλιστεί και εκπαιδευτεί από τις Βρετανικές μυστικές υπηρεσίες (SAS). Το γεγονός αυτό είναι άκρως αποκαλυπτικό για το πώς προετοιμάζονται οι "ανθρωπιστικοί" πόλεμοι, αλλά συνδέεται και με τις γενικότερες εξελίξεις στη Μέση Ανατολή. Βλέπετε, όταν το έργο της SAS ολοκληρώθηκε στη Λιβύη, ένα κλιμάκιό της αναχώρησε για τη Συρία...

Η νέα "μεγάλη απειλή για την ανθρωπότητα" είναι εδώ. Φωτίζοντας ένα μόνο μέρος της πραγματικότητας --την αθλιότητα και τη βαρβαρότητα των Τζιχαντιστών--, τα ΜΜΕ πετυχαίνουν το σκοπό τους: Προετοιμάζουν την κοινή γνώμη για τον επόμενο πόλεμο στο Ιράκ και στη Συρία. Ταυτόχρονα, προλειαίνεται και το έδαφος για την εφαρμογή νέων αντιτρομοκρατικών νόμων στην ΕΕ, με πρόσχημα τη λεγόμενη "πάλη κατά του εξτρεμισμού". Εσείς τι καταλαβαίνετε από όλα αυτά; Ποιοι θα είναι τα θύματα του επόμενου πολέμου; Πόσοι και ποιοι θα σκοτωθούν; Πόσο θα στοιχίσει η συμμετοχή μας, που αν γίνει πόλεμος είναι σίγουρη; Και, σε τελική ανάλυση, τι εννοούν όταν μιλάνε για αντιτρομοκρατικούς νόμους, αυτοί που έχουν εκπαιδεύσει τους πιο στυγνούς δολοφόνους;

Αχ, αυτή η δροσιά! Μόλις φύσηξε λίγο, ηρέμησα και χαλάρωσα. Δεν ξέχασα αυτά που σας έγραψα παραπάνω, ούτε τα θεωρώ δευτερεύοντα ζητήματα. Θυμήθηκα όμως ότι έχουμε μπει στο Φθινόπωρο και, υπό μία έννοια, έχουμε μπροστά μας μια νέα χρόνια. Η ενημέρωση που δεχόμαστε από τα ΜΜΕ δεν θα αλλάξει χαρακτήρα, αλλά εμείς μπορούμε ν' αλλάξουμε την αντίληψη και τη στάση μας. Να ξέρετε ότι από κοντά θα αλλάξει και το αγαπημένο μας περιοδικό, το οποίο συμβάλλει στην ουσιαστική ενημέρ[redacted]

ΛΟΓΟΚΡΙΝΕΤΑΙ

...Περισσότερα όμως στο επόμενο τεύχος ;)



σνέιλ μέιλ

Αγαπητοί μου,

Καθισμένος όπως είμαι στον ξύλινο πάγκο της αυλής, δίπλα στη μεγάλη αιώρα, πρέπει να το παραδεχτώ. Ο ήχος αυτός μου είχε λείψει.

Ο ήχος των τζιτζικιών.

Δεν το συνειδητοποιείς πόσο σημαντικό κομμάτι του καλοκαιριού είναι, παρά μόνον όταν απουσιάζει. Στο Λονδίνο, ας πούμε, που ήμουν τους τελευταίους δύο μήνες με τον ανιψιό, ακούς τα πάντα, αλλά τζιτζίκια δεν ακούς. Φέτος μάλιστα που ο καιρός ήταν πιο μεσογειακός από κάθε άλλη φορά, η έλλειψη ήταν πιο χτυπητή.

Ήλιος, ντάλα να σε χτυπάει, τριαντάρια στο θερμόμετρο, νόμιζες πως είσαι στην Κέρκυρα.

Κέρκυρα: Πράσινο, υγρασία, ήλιος, Άγγλοι. Το πλήρες πακέτο.

Αλλά κάτι να λείπει.

Ε, λοιπόν, κάποια στιγμή το κατάλαβα. Έλειπαν τα τζιτζίκια.

Με το που επιστρέψαμε, απέτυχα να ολοκληρώσω κάτι εκκρεμότητες που είχα με δημόσιες υπηρεσίες --θα μου επιτρέψετε, αγαπητοί μου, να μην επεκταθώ επ' αυτού-- και μετά ήρθα σούμπιτος στο Πόρτο Γερμενό.

Είμαι εδώ από τις αρχές του μήνα και το μόνο που κάνω είναι να κάθομαι στον ξύλινο πάγκο, δίπλα στη μεγάλη αιώρα. Στην αιώρα την ίδια δεν ανεβαίνω. Κάθομαι στον πάγκο, κοιτάω την θάλασσα, και ακούω τα τζιτζίκια.

Από προχτές πλάκωσαν και οι υπόλοιποι. Τώρα που σας γράφω είναι όλοι καθισμένοι κάπου εδώ γύρω και τρώνε καρπούζι.

Βέβαια αυτά που σας λέω άμα θέλετε τα πιστεύετε. Τα λέγαμε, να μην τα ξαναλέμε. Ο βαθμός αληθείας των προτάσεών μου είναι απροσδιόριστος. Μπορεί να είναι αληθείς, μπορεί και όχι. Και αυτό δεν έχει μόνο να κάνει με την άγνοιά μας. Είναι αποτέλεσμα της εγγενούς ασάφειας της γλώσσας.

Κάπου διάβαζα ότι υπάρχει ένας κλάδος της λογικής που δέχεται (και αξιοποιεί) τέτοιες αμφίσημες προτάσεις, τις οποίες ονομάζει δι-αλήθειες. Είχα μάλιστα σκεφτεί να σας γράψω για αυτές τις δι-αλήθειες --στα αγγλικά dialetheias-- αλλά είχαμε νωρίτερα σήμερα μιαν ενδιαφέρουσα, φιλοσοφίζουσα (ελαφρώς) συζήτηση με τους υπολοίπους, και σκέφτομαι να σας μεταφέρω κάποια χάι-λάιτ.

Τη συζήτηση την ξεκίνησε η μητέρα της εξαδέλφης: "Διάβαζα τις επιστολές σου σ' εκείνο το περίεργο περιοδικό που γράφεις."

"Ε όχι και περίεργο--" πήγα να διαμαρτυρηθώ.

"Δεν γράφεις πλέον για πολιτικά, παρατηρώ", συνέχισε ακάθεκτη εκείνη.

"Αφήστε τον καλέ μαμά, τι τον τσιγκλάτε κι εσείς τώρα. Να αρχίσει πάλι να γράφει και να του την πέσουν ξανά από τη γωνία να τον φάνε; Δεν είδατε τι του λέγανε;" μπήκε στην κουβέντα η εξαδέλφη.

Εγώ ξεφύσηξα στεναχωρημένος. Δεν είπα τίποτα.

"Άλλο με ενδιαφέρει εμένα", είπε η μητέρα της εξαδέλφης, που είναι ινδουίστρια. "Ούτε τα πολιτικά, ούτε τα κολλήματα του καθενός. Εγώ προσπαθώ να καταλάβω τι εννοούσες με αυτά που έλεγες για το 'είναι'. Πες μου. Τι θα πει να αναρωτιέσαι, 'τι σημαίνει "είναι";' Αν κάτι 'είναι', τότε είναι. Ποιο είναι το πρόβλημά σου;"

Οι υπόλοιποι σταμάτησαν ό,τι έκαναν (δηλαδή να χαζεύουν τη θάλασσα) και γύρισαν προς το μέρος μας.

"Κοιτάχτε", είπα εγώ διστακτικά, "αυτό που προσπαθούσα να επισημάνω είναι πως αυτή η λέξη, η λέξη 'είναι', δεν είναι τόσο διαφανής και ουδέτερη όσο θα θέλαμε. Περιλαμβάνει πάντα μιαν οπτική γωνία. Μια 'θεωρία', για να το πω και αλλιώς."

"Τα μπερδεύεις", παρενέβη από την άλλη ο ανεπρόκοπος. "Άλλο θεωρία, άλλο οπτική γωνία."

"Ανιψιέ μην πετάγεσαι!" τον αποπήρα εγώ. "Δεν μπερδεύω τίποτα."

"Δηλαδή τι εννοείς;" επέμεινε η μητέρα της εξαδέλφης.

"Να. Ας πούμε ότι λέω: 'Το ηλιοβασίλεμα στο Πόρτο Γερμενό είναι όμορφο'. Δεν τη βλέπετε εδώ την οπτική γωνία;"

"Χα", κάγχασε ο ανιψιός.

"Νομίζω ότι το μαγειρεύεις λίγο", είπε η εξαδέλφη. "Παίζεις με τις λέξεις. Άλλο είναι να λες για το ηλιοβασίλεμα και άλλο, ξέρω 'γω να μιλάς για κάτι άλλο, αντικειμενικό."

"Τι θα θεωρούσες εσύ αντικειμενικό;"

"Αντικειμενικό θέλεις;" λέει ο ανιψιός. "Ορίστε: 'Ο χρόνος ημιζωής του πλουτώνιου-238 είναι 87,7 χρόνια'. Πού είναι η οπτική γωνία εδώ;"

"Δεν τη βλέπεις;", του λέω εγώ. "Μιλάς για χρόνο. Ο παρατηρητής είναι εντός χρόνου ή εκτός; Με αναφορά σε ποιόν παρατηρητή μετράμε τον χρόνο;"

"Άστα αυτά", μου λέει ο ανιψιός. "Η μέτρηση εξαρτάται από το σύστημα αναφοράς στο οποίο βρίσκεται ο παρατηρητής, ναι, αλλά μέσα σε κάθε δεδομένο σύστημα η μέτρηση είναι αντικειμενική. Δεν είναι όπως το ηλιοβασίλεμα. Η διαδικασία της ραδιενεργού διάσπασης λαμβάνει χώρα ανεξαρτήτως του παρατηρητή. Δεν είναι στο χέρι του παρατηρητή να αποφασίσει τι θα μετρήσει. Θα μετρήσει 87,7 χρόνια ή κάτι άλλο (ανάλογα με το σύστημα



αναφοράς), αλλά δεν είναι στο χέρι του να μετρήσει πότε το ένα και πότε το άλλο. Αν πούμε ότι κάτι 'είναι' έτσι ή 'είναι' αλλιώς, το μόνο που κάνουμε είναι να αποτυπώνουμε κάποια πλευρά της διαδικασίας αυτής σε μια πρόταση. Το ίδιο το 'είναι' είναι διαφανές."

Αγαπητοί μου,

Όπως βλέπετε, η συζήτησή μας είχε ανέβει πολύ γρήγορα σε διανοητικά ύψη δυσθεώρητα. Ο χώρος δεν μου επιτρέπει να σας μεταφέρω εδώ όλες τις λεπτές αποχρώσεις του διαλόγου. Δεν μου φτάνει καν για να διατυπώσω με επάρκεια το επιχείρημά μου. Θα προσπαθήσω, όμως, να δώσω ένα πρώτο περίγραμμά του. Όσο χωρέσει.

Η ουσία, λοιπόν, είναι πως στο παράδειγμα των "ουδέτερων" προτάσεων σαν αυτή για το πλουτώνιο-238, υπάρχει μεν αυτό που έχουμε συνηθίσει να ονομάζουμε αντικειμενικότητα ή διαφάνεια, αλλά αυτή η διαφάνεια δεν υπήρχε εξ αρχής. Πρόκειται πάντα για αποτέλεσμα αφαίρεσης, abstraction. Πάντα ξεκινάμε από κάτι που δεν είναι καθόλου "αντικειμενικό" και στη συνέχεια το καθιστούμε όλο και πιο αφηρημένο, μέχρι που ψηνόμαστε τελικά πως είναι "αντικειμενικό".

Το επιχείρημά μου είναι πως η υποτιθέμενη "αντικειμενικότητά" μας είναι πάντα προϊόν μιας υποκειμενικότητας. Το ξεχνάμε, όμως, και νομίζουμε ότι τα πράγματα ξεκινούν αλλιώς, πως η σκέψη μας στέκεται απέναντι στον κόσμο σαν σ' ένα δίπολο: από τη μία η σκέψη, από την άλλη το "αντικείμενο". Θεωρούμε πως η υποκειμενικότητα είναι παρείσακτος, πρόβλημα, παράσιτο που πρέπει να ξεριζωθεί, ενώ δεν είναι καθόλου έτσι. Ουσιαστικά ακόμα και οι έννοιες που χρησιμοποιούμε --"αντικειμενικότητα", "υποκειμενικότητα" κ.λπ.-- είναι προβληματικές επειδή εμπεριέχουν --και αντικατοπτρίζουν-- την ίδια αρχική πεποίθηση πως η σκέψη βρίσκεται σε θέση ουδέτερου παρατηρητή ως προς τον κόσμο.

Η πεποίθηση αυτή είναι προβληματική.

Πάρτε, ας πούμε, όλες τις προσπάθειες να σχεδιαστούν αλγοριθμικά μοντέλα της ανθρώπινης σκέψης. Όλες έχουν την ίδια αφετηρία. Ο ανθρώπινος εγκέφαλος που στέκεται "απέναντι" στον κόσμο, προσλαμβάνει δεδομένα από τα αισθητήρια όργανα, τα επεξεργάζεται, τα κατηγοριοποιεί, τα αποθηκεύει και τα ανακαλεί, διαμορφώνει και τροποποιεί προγράμματα δράσης και λοιπά και λοιπά.

Προσπαθούμε λοιπόν να φτιάξουμε αλγορίθμους που να κάνουν το ίδιο και αποτυγχάνουμε οικτρά. Δεν αναρωτιέστε γιατί;

Αποτυγχάνουμε γιατί παίρνουμε ως δεδομένο πως η "αντικειμενικότητα", whatever that is, είναι θεμέλιο της ανθρώπινης σκέψης, ενώ δεν είναι παρά προϊόν της προσπάθειάς μας να περιγράψουμε το πώς εμπλεκόμαστε, εμείς οι άνθρωποι, στον κόσμο. Ένα προϊόν ιστορικό.

'Όταν λέω ιστορικό προϊόν, εννοώ πως η εικόνα που έχουμε σήμερα για την ανθρώπινη σκέψη είναι προϊόν της νεωτερικής εποχής, της εποχής που εγκαινιάζεται με τον Γαλιλαίο. Η εικόνα αυτή διαφέρει θεμελιωδώς από εκείνη που είχαν για την ανθρώπινη σκέψη οι αρχαίοι Ελληνες, οι Ινδοί ή οι Κινέζοι. Δεν είναι καλύτερη ή χειρότερη, σωστότερη ή πιο λάθος. Απλά *διαφέρει*.

Ας μείνουμε προς το παρόν εδώ. Ο χώρος δεν επαρκεί για να το αναπτύξω αυτό περισσότερο. Σταματώ αλλά θα επιστρέψω. Όμως πρώτα έχω ένα ερώτημα για σας.

Ξεκίνησα γράφοντας για τα τζιτζίκια. Για μένα κάτι λείπει από τον ήχο του καλοκαιριού αν δεν έχει τζιτζίκια. Πείτε μου, λοιπόν. Ακούγεται το "τζι τζι" των τζιτζικιών αν δεν είμαστε εμείς εκεί να το ακούσουμε;

Σας ασπάζομαι,
Θείος Ακάκιος

Skill: Intermediate
Tags: dSploit, wifi cracker, port scan, traceroute, brute force, dictionary attacks, MiTM attacks

dSploit



by Tom Cr0w

Hacking με το Android [part 1]

Το Android το χρησιμοποιούμε καθημερινά, για να επικοινωνήσουμε, για να διασκεδάσουμε κι ορισμένες φορές για να εκτονώσουμε το καλλιτεχνικό μας μεράκι. Τι θα λέγατε αν το αξιοποιούσαμε και σε ένα από τα αγαπημένα μας hobby; Αναφερόμαστε στο Penetration Testing, όπου το Android μπορεί να φανεί εξαιρετικά χρήσιμο! Σε αυτό το μέρος της σειράς θα γνωρίσουμε το πανίσχυρο dSploit...

Η αγορά των smartphones είναι τόσο ανεπτυγμένη που όλοι σχεδόν οι γνωστοί και οι φίλοι μας διαθέτουν ένα τέτοιο τηλέφωνο —ακόμα κι οι γονείς μας, δηλαδή! Στα δικά μας μάτια, βέβαια, αυτό που καθιστά ιδιαίτερα ενδιαφέρουσες τις συγκεκριμένες συσκευές δεν σχετίζεται με το μερίδιο αγοράς που έχουν κατακτήσει, ούτε με κάποιον άλλο οικονομοτεχνικό παράγοντα. Το ζουμί της υπόθεσης βρίσκεται στην επεξεργαστική ισχύ των smartphones. Είτε το συνειδητοποιούμε είτε όχι, οι περισσότεροι από εμάς κυκλοφορούμε μ' ένα ολοκληρωμένο σύστημα στην τσέπη, που κατά πάσα πιθανότητα διαθέτει επεξεργαστή ARM χρονισμένο στα 2,5GHz, 2GB μνήμης RAM και τουλάχιστον 16GB "εσωτερικού" αποθηκευτικού χώρου. Όπως αντιλαμβάνεστε, μιλάμε για συστήματα που θα μπορούσαν να σηκώσουν την αγαπημένη μας διανομή Linux με άνεση και να μας συντροφεύουν επάξια σε πολλές από τις υπολογιστικές μας περιπέτειες. Μα, τι λέμε; Τα περισσότερα smartphones τρέχουν ήδη Linux! Τι θα λέγατε λοιπόν αν εγκαθιστούσαμε τα κατάλληλα προγράμματα, ώστε να μετατρέψουμε ένα smartphone με Android σ' ένα πανίσχυρο εργαλείο για pen testing;

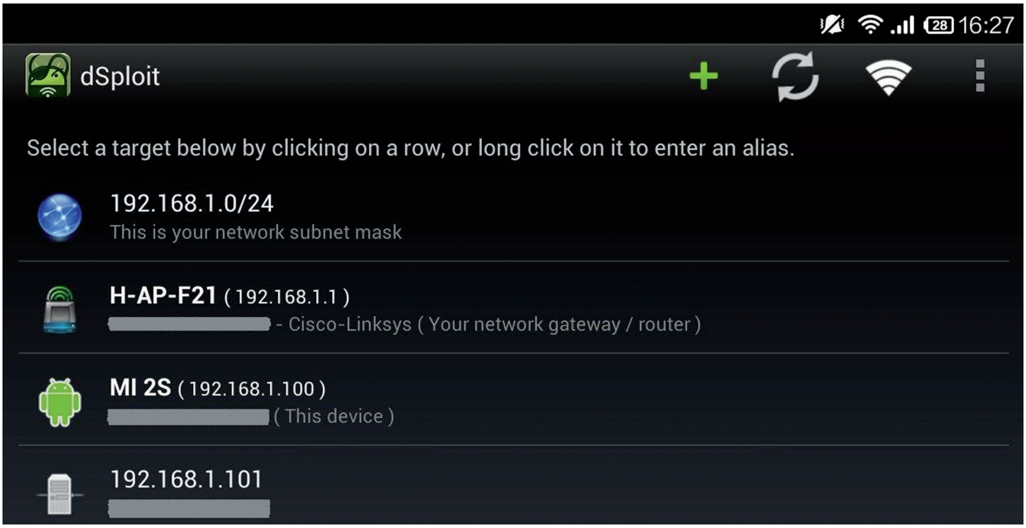
Παρόμοιες σκέψεις έχουν κάνει πολλοί developers, εδώ κι αρκετό καιρό. Έτσι, αν θέλουμε να τσεκάρουμε την ασφάλεια ενός router, ενός δικτύου ή και κάποιας υπηρεσίας, δεν χρειάζεται πλέον να κουβαλάμε το laptop. Μπορούμε να κάνουμε τις σχετικές δοκιμές από το smartphone, αφού προηγουμένως εγκαταστήσουμε τις κατάλληλες εφαρμογές. Σ' αυτή τη μίνι σειρά άρθρων θα εξετάσουμε ορισμένες από τις πιο ισχυρές και αξιόλογες εφαρμογές του είδους, ξεκινώντας από το περίφημο dSploit.

Απαραίτητες διευκρινίσεις

Πριν προχωρήσουμε οφείλουμε να σταθούμε σε ορισμένες κρίσιμες λεπτομέρειες. Κατ' αρχάς, για την ομαλή και απρόσκοπτη λειτουργία των προγραμμάτων που θα παρουσιάσουμε, η συσκευή μας θα πρέπει να είναι rooted. Η διαδικασία για να πετύχουμε κάτι τέτοιο δεν είναι ίδια για όλες τις συσκευές, αλλά δεν αποτελεί το θέμα του παρόντος. Αν θέλετε να εγκαταστήσετε τις εφαρμογές που θα παρουσιάσουμε αλλά η συσκευή σας δεν είναι rooted, μπορείτε να ξεκινήσετε τη μελέτη από το σχετικό άρθρο στο τεύχος 004 του περιοδικού.

Η αποτελεσματικότητα των εφαρμογών που θα παρουσιάσουμε δεν επηρεάζεται από τα γενικά χαρακτηριστικά της συσκευής μας. Αντίθετα, η ταχύτητά τους καθορίζεται σε τεράστιο βαθμό από τις επιδόσεις του επεξεργαστή και την έκταση της μνήμης. Αυτό είναι αυτονόητο, θα πουν πολλοί, αλλά πρέπει να το τονίσουμε. Βλέπετε, ορισμένες λειτουργίες θα μοιάζουν να μην εξελίσσονται καθόλου, όταν τις εκτελούμε σε παλιά smartphones...

Πολλές φορές, οι εφαρμογές διαχείρισης δικαιωμάτων, όπως το SuperSU, εισάγουν καθυστερήσεις στη λειτουργία των προγραμμάτων. Αυτό συμβαίνει γιατί ορισμένα προγράμματα ζητούν δικαιώματα root ξανά και ξανά, σε τακτά χρονικά διαστήματα. Για να περιορίσουμε —αν όχι να αποφύγουμε— αυτό το πρόβλημα, πρέπει να χρησιμοποιούμε πάντα την τελευταία έκδοση της εφαρμογής διαχείρισης δικαιωμάτων και να παρέχουμε πλήρη δικαιώματα στην εφαρμογή με την οποία πρόκειται να εργαστούμε, χωρίς επανέλεγχο. Τέλος, εξετάζοντας το πώς μπορούμε να μετατρέψουμε ένα σύστημα με Android σε σταθμό εργασίας για pen testing, δεν θα έπρεπε να παραλείψουμε το BusyBox. Πρόκειται για ένα πακέτο που ενσωματώνει περικομμένες εκδοχές *όλων* των βασικών εργαλείων που διαθέτει μια τυπική εγκατάσταση Linux. Με μια αναζήτηση στο PlayStore θα βρείτε πολλούς installers για το BusyBox.

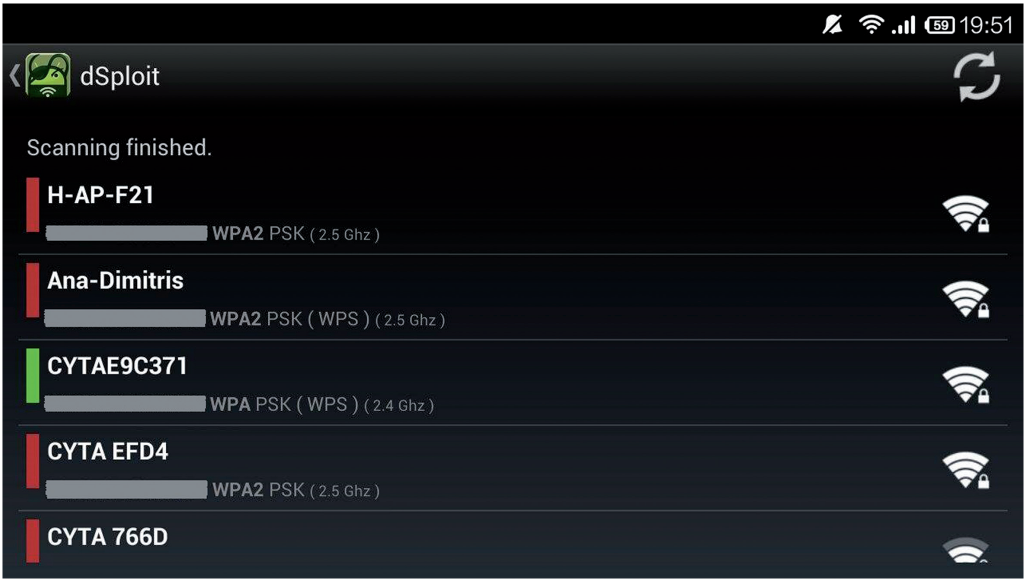


Αυτή είναι η κεντρική "περιοχή" του dSploit. Στο πάνω δεξιό μέρος της εφαρμογής βλέπουμε τις εξής λειτουργίες: Προσθήκη διεύθυνσης ή URL ενός νέου στόχου, εκκίνηση νέας σάρωσης του δικτύου για συσκευές, εκκίνηση του WiFi Cracker και εμφάνιση ρυθμίσεων. Στο κυρίως τμήμα του παραθύρου της εφαρμογής βλέπουμε τις συσκευές που έχουν εντοπιστεί στο ασύρματο δίκτυο...

Το περίφημο dSploit

Η πρώτη εφαρμογή που θα εξετάσουμε θα μπορούσε να χαρακτηριστεί κι ως ελβετικός σουγιάς, αφού προσφέρει υπερβολικά πολλές λειτουργίες. Μάλιστα, θα τολμούσαμε να πούμε ότι οι περισσότερες από αυτές υλοποιούνται με υποδειγματικό τρόπο! Η εφαρμογή δημιουργήθηκε αρχικά από τον διάσημο, τώρα πια, evilsocket, αλλά με το πέρας του χρόνου προστέθηκαν κι άλλοι developers. Το dSploit διατίθεται υπό την άδεια GNU GPL3. Αυτό σημαίνει ότι ο κώδικάς του είναι ανοικτός και μπορεί ο καθένας να τον τροποποιήσει και να τον αναδιανείμει δωρεάν ή επί πληρωμή. Η παραπάνω διευκρίνιση μπορεί να μοιάζει περιττή, αλλά αν κάνετε μια αναζήτηση στο PlayStore θα διαπιστώσετε ότι υπάρχουν πολλές εφαρμογές με το όνομα dSploit. Η αυθεντική εκδοχή του προγράμματος παρέχεται από το δικτυακό τόπο `http://dSploit.net` και θα σας προτείναμε να χρησιμοποιήσετε αυτόν και όχι κάποιον από το PlayStore.

Αν μεταβούμε στο δικτυακό τόπο του προγράμματος και συγκεκριμένα στην "καρτέλα" Download, θα βρούμε δύο εκδόσεις: Τη βασική κι εκείνη με τον χαρακτηρισμό "Nightly Build". Εμείς θα χρησιμοποιήσουμε τη βασική, που διαθέτει λιγότερα bugs και σε γενικές γραμμές είναι αρκετά πιο σταθερή. Η μόνη ουσιαστική διαφορά μεταξύ των δύο εντοπίζεται στην παρουσία του Metasploit Framework. Ωστόσο, η ενσωμάτωση του εν λόγω πακέτου βρίσκεται σε πολύ πρώιμο στάδιο. Με αυτά τα δεδομένα, λοιπόν, κατεβάζουμε από τον browser της συσκευής μας το αρχείο APK με τη βασική έκδοση του dSploit. Τη στιγμή που γραφόταν το άρθρο, η νεότερη έκδοση του προγράμματος ήταν η 1.0.31b. Στη συνέχεια, αν δεν το έχουμε κάνει ήδη, πρέπει να επισκεφθούμε τις ρυθμίσεις της συσκευής μας και να επιτρέψουμε την εγκατάσταση εφαρμογών από άγνωστες πηγές. Με αυτή τη ρύθμιση θα μπορούμε να εγκαταστή-



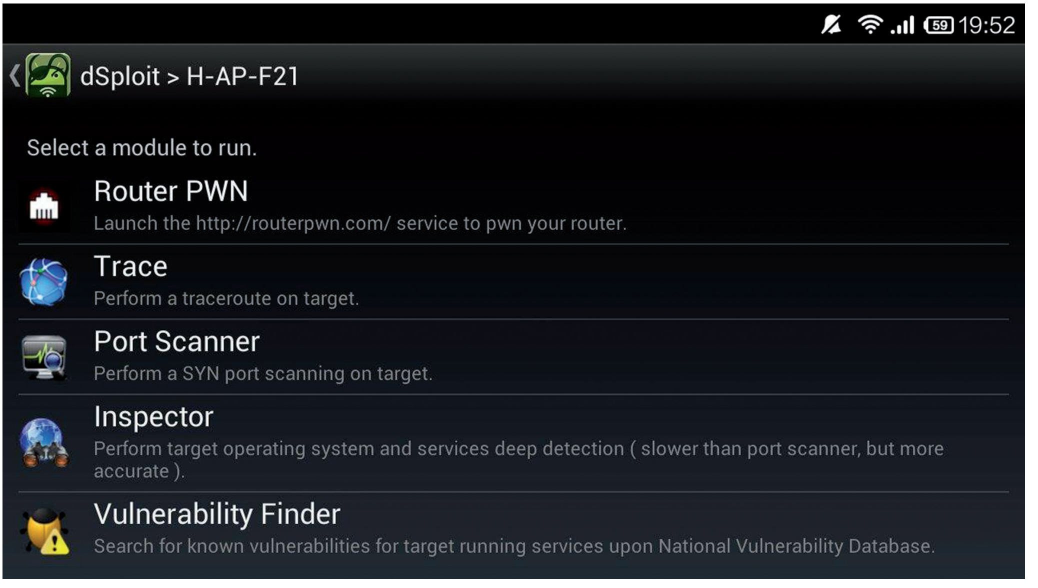
Το περιβάλλον του WiFi Cracker. Με πράσινο αναφέρονται οι συσκευές που είναι ευάλωτες σε κάποια τεχνική αποκάλυψης του εργοστασιακού κλειδιού ασφαλείας. Με κόκκινο αναφέρονται οι (σχετικά) ασφαλείς συσκευές, για τις οποίες είναι αδύνατο να υπολογιστεί αυτόματα το κλειδί.

σουμε το πακέτο APK που κατεβάσαμε, χωρίς το παραμικρό πρόβλημα. Τέλος, πρέπει να ανοίξουμε την εφαρμογή διαχείρισης δικαιωμάτων που έχουμε εγκατεστημένη (εμείς χρησιμοποιούμε το SuperSU) και να δώσουμε στο dSploit πλήρη πρόσβαση και χωρίς επανέλεγχο. Μετά από τα παραπάνω, μπορούμε επιτέλους να ξεκινήσουμε την εφαρμογή…

WiFi cracker

Κάθε φορά που εκτελούμε την εφαρμογή πραγματοποιείται ένας έλεγχος για το αν είμαστε συνδεδεμένοι σε κάποιο ασύρματο δίκτυο[1]. Αν συμβαίνει κάτι τέτοιο, ξεκινάει αυτόματα ένα network scanning που σε ελάχιστο χρόνο εμφανίζει το πλήθος και το είδος των συσκευών που είναι συνδεδεμένες στο ίδιο δίκτυο. Αν δεν είμαστε συνδεδεμένοι, το πρόγραμμα εμφανίζει επάνω και δεξιά μια επιλογή με το σηματάκι του WiFi. Πρόκειται για έναν WiFi Cracker! Αν κάνουμε κλικ στο εικονίδιο θα ξεκινήσει μια σάρωση για τον εντοπισμό των διαθέσιμων ασύρματων δικτύων. Στο τέλος το πρόγραμμα θα εμφανίσει μια λίστα με τα εντός εμβέλειας δίκτυα, στην οποία κάποια θα εμφανίζονται με κόκκινο χρώμα και κάποια με πράσινο. Τα δίκτυα που παρουσιάζουν το περισσότερο ενδιαφέρον είναι αυτά με το πράσινο χρώμα, αφού υπάρχει η πιθανότητα να βρεθεί ο κωδικός ασφαλείας. Η σχετική επίθεση στηρίζεται σε γνωστούς αλγόριθμους για την παραγωγή των εργοστασιακών κλειδιών των ρούτερ. Η λίστα με τις υποστηριζόμενες συσκευές είναι μεγάλη και περιλαμβάνει μοντέλα από την Thomson και την DLink, καθώς και πολλούς ακόμα κατασκευαστές.

1. Το dSploit λειτουργεί μόνο σε συνδέσεις ασύρματου δικτύου (IEEE 802.11-WLAN) και όχι σε συνδέσεις Cellular.



Η "σελίδα" που βλέπουμε όταν επιλέξουμε κάποιον στόχο. Εδώ φαίνονται όλες οι λειτουργίες που προσφέρει το dSploit. Η φωτογραφία είναι από τη "σελίδα" που εμφανίζει το πρόγραμμα για κάποιον router/ network getaway και περιλαμβάνει το εργαλείο RouterPwn!

Υποψήφιοι στόχοι

Αφού συνδεθούμε σε κάποιο ασύρματο δίκτυο και μετά από την ολοκλήρωση του network scanning που πραγματοποιείται αυτόματα, εμφανίζεται μια λίστα με τους πιθανούς στόχους — τα συστήματα που είναι συνδεδεμένα στο ίδιο δίκτυο. Σημειώστε ότι η πρώτη καταχώριση αυτής της λίστας δεν αποτελεί συσκευή, αλλά πρόκειται για το subnet mask του δικτύου. Οι επιλογές που προσφέρει το dSploit για αυτή την καταχώριση περιλαμβάνουν μόνο τις επιθέσεις Man-in-The-Middle, στις οποίες θα αναφερθούμε αργότερα.

Στη δεύτερη γραμμή της λίστας εμφανίζεται η συσκευή του ρούτερ ή, αλλιώς, η πύλη δικτύου (network gateway). Η πιο ενδιαφέρουσα από τις λειτουργίες που προσφέρονται εδώ είναι το λεγόμενο RouterPwn. Επιλέγοντάς το μεταφερόμαστε στο `http://routerpwn.com`, μέσω του προεπιλεγμένου browser της συσκευής. Εκεί θα βρούμε μια δικτυακή εφαρμογή που περιέχει όλα τα γνωστά exploits για την κατάληψη ενός ρούτερ, δηλαδή για την απόκτηση πρόσβασης με πλήρη δικαιώματα.

Εκτός από τους στόχους που εμφανίζονται στη λίστα του dSploit, ενδέχεται να υπάρχουν και συσκευές που καταφέρνουν να κρυφτούν από το scanning της εφαρμογής. Φυσικά, το dSploit παρέχει λύση και γι' αυτό το προβληματάκι. Στο πάνω δεξιό τμήμα της εφαρμογής εμφανίζεται ένα κουμπάκι με το σύμβολο της πρόσθεσης. Πατώντας το μπορούμε να προσθέσουμε χειροκίνητα τη διεύθυνση IP οποιουδήποτε συστήματος κρύφτηκε από την αυτόματη ανίχνευση ή ακόμα και κάποιο URL, που γνωρίζουμε ότι παραπέμπει σε κάποια κρυμμένη συσκευή. Όπως αντιλαμβάνεστε, η συγκεκριμένη λειτουργία του dSploit επιτρέπει να προσθέσουμε και στόχους εκτός του ασύρματου δικτύου :D

Κύριος οπλισμός

Μέχρι στιγμής έχουμε αναφερθεί σε ορισμένες περιφερειακές/βοηθητικές λειτουργίες που προσφέρει το πρόγραμμα. Δεν έχουμε πει τίποτα ακόμα για το κυρίως οπλοστάσιο του DSpoit, από το οποίο απορρέει και η μεγάλη του χρησιμότητα. Κάπου εδώ, όμως, νομίζουμε ότι το έχουμε παρακάνει με τους προλόγους. Στη συνέχεια θα εξετάσουμε μία προς μία τις βασικές λειτουργίες του προγράμματος.

Trace. Με τη βοήθεια αυτού του εργαλείου μπορούμε να τσεκάρουμε την πορεία που ακολουθούν τα πακέτα δεδομένων που εκπέμπουμε, μέχρι να φτάσουν στον εκάστοτε προορισμό. Με λίγα λόγια, η επιλογή trace πραγματοποιεί το λεγόμενο traceroute.

Port Scanner. Οι περισσότερες επιθέσεις ξεκινούν με ένα port scanning, ώστε να μάθουμε πόσα και ποια δικτυακά ports είναι ανοιχτά σε κάποιο σύστημα. Με αυτή τη γνώση μπορούμε να κάνουμε μια πρώτη εκτίμηση για τις υπηρεσίες που εκτελούνται στο υπό εξέταση σύστημα. Στη συνέχεια, αξιοποιώντας και αυτό το εφόδιο, μπορούμε να εξειδικεύσουμε την περαιτέρω εξέταση του στόχου — ή ακόμα και την επίθεση.

Όταν ολοκληρώνεται το port scanning, το πρόγραμμα εμφανίζει μια λίστα με τα ανοικτά ports. Εμείς μπορούμε να επιλέξουμε κάποιο από αυτά και να επιχειρήσουμε να συνδεθούμε. Αν το επιλεγμένο port χρησιμοποιείται για το "σερβίρισμα" περιεχομένου web, to dSploit θα επιχειρήσει να συνδεθεί με τον προεπιλεγμένο browser.



Αφού έχουμε εντοπίσει τα ανοικτά ports του στόχου μπορούμε να ξεκινήσουμε τον Inspector. Όπως φαίνεται στην εικόνα, ο Inspector εμφανίζει διάφορες πληροφορίες για το στόχο, όπως το λειτουργικό σύστημα και οι υπηρεσίες (services) που εκτελούνται.

Σε διαφορετική περίπτωση θα επιχειρήσει να ξεκινήσει μια σύνδεση telnet. Αν και τα παραπάνω μπορεί να ακούγονται εξαιρετικά απλοϊκά έως και αδιάφορα, σημειώστε ότι η διενέργεια ενός port scanning αποτελεί απαραίτητη προϋπόθεση για τη χρήση του Inspector και μετέπειτα του Vulnerability Finder.

Inspector. Η συγκεκριμένη λειτουργία πραγματοποιεί μια πιο σχολαστική διερεύνηση του στόχου, για την αποκάλυψη του λειτουργικού συστήματος και των υπηρεσιών που εκτελούνται. Παρεμπιπτόντως, χρησιμοποιώντας αυτή τη λειτουργία στην ίδια τη συσκευή μας, μπορούμε να μάθουμε πόσο ευάλωτο είναι το σύστημά μας, όπως επίσης και το πόσα στοιχεία θα μπορούσε να συλλέξει κανείς για εμάς! Η εκτέλεση του Inspector αποτελεί αναγκαίο βήμα, αν σκοπεύουμε να προχωρήσουμε περισσότερο και να ψάξουμε για τυχόν κενά στην ασφάλεια του συστήματος-στόχου.

Vulnerability Finder. Η συγκεκριμένη λειτουργία αξιοποιεί όλα τα δεδομένα που έχουν συγκεντρωθεί από το port scanning και την εκτέλεση του Inspector, σε συνδυασμό με τα περιεχόμενα της βάσης CVSS (Common Vulnerability Scoring System). Ως γνωστόν, πρόκειται για μία βάση δεδομένων που περιέχει χρήσιμες πληροφορίες για όλες τις γνωστές ευπάθειες, όπως το πώς εκδηλώνονται, σε ποιες εκδόσεις ποιων υπηρεσιών, σε ποια λειτουργικά συστήματα κ.λπ. Τελικά, η λειτουργία του Vulnerability Finder έχει σαν αποτέλεσμα τη συγκρότηση μιας λίστας με όλες τις ευπάθειες που ενδέχεται να υπάρχουν στο στόχο μας, καθώς και μία σύντομη περιγραφή της καθεμίας. Επιλέγοντας μια ευπάθεια, το πρόγραμμα μάς μεταφέρει στην αντίστοιχη σελίδα του National Vulnerability Database, που φιλοξενείται στο NIST (http://nvd.nist.gov). Από εκεί μπορούμε να μάθουμε περισσότερα για την κρισιμότητα της επιλεγμένης ευπάθειας, καθώς και για τις πιθανές λύσεις.

Login Cracker. Το dSploit περιλαμβάνει τον δικό του Login Cracker, που μπορεί να εκτελεί επιθέσεις brute-force, όπως επίσης και dictionary attacks. Για την πραγματοποίηση μιας επίθεσης brute-force αρκεί να επιλέξουμε την υπηρεσία στην οποία θέλουμε να επιτεθούμε (FTP, HTTP-Head, ICQ και πολλές ακόμα), καθώς και το σχετικό port. Κατόπιν, εισάγουμε το username που θέλουμε να χρησιμοποιηθεί κατά την επίθεση κι ορίζουμε το άνω όριο για το μέγεθος των passwords. Η επίθεση ξεκινά με ένα πάτημα του κουμπιού Start! Εξίσου απλά είναι τα πράγματα και με τα dictionary attacks: Επιλέγουμε την επιθυμητή υπηρεσία και το αντίστοιχο port, ενώ στη συνέχεια δίνουμε στο πρόγραμμα ένα wordlist με τα πιθανά usernames (User Wordlist) κι ένα ακόμα με τα πιθανά passwords (Password Wordlist). Για την εκτέλεση της επίθεσης πατάμε και πάλι το κουμπί Start.

Packet Forger. Αυτή η λειτουργία μπορεί να φανεί χρήσιμη σε πολύ προχωρημένες επιθέσεις. Όπως δηλώνει και το όνομά της, επιτρέπει το σχηματισμό πακέτων TCP ή UDP και την αποστολή τους στο θύμα.

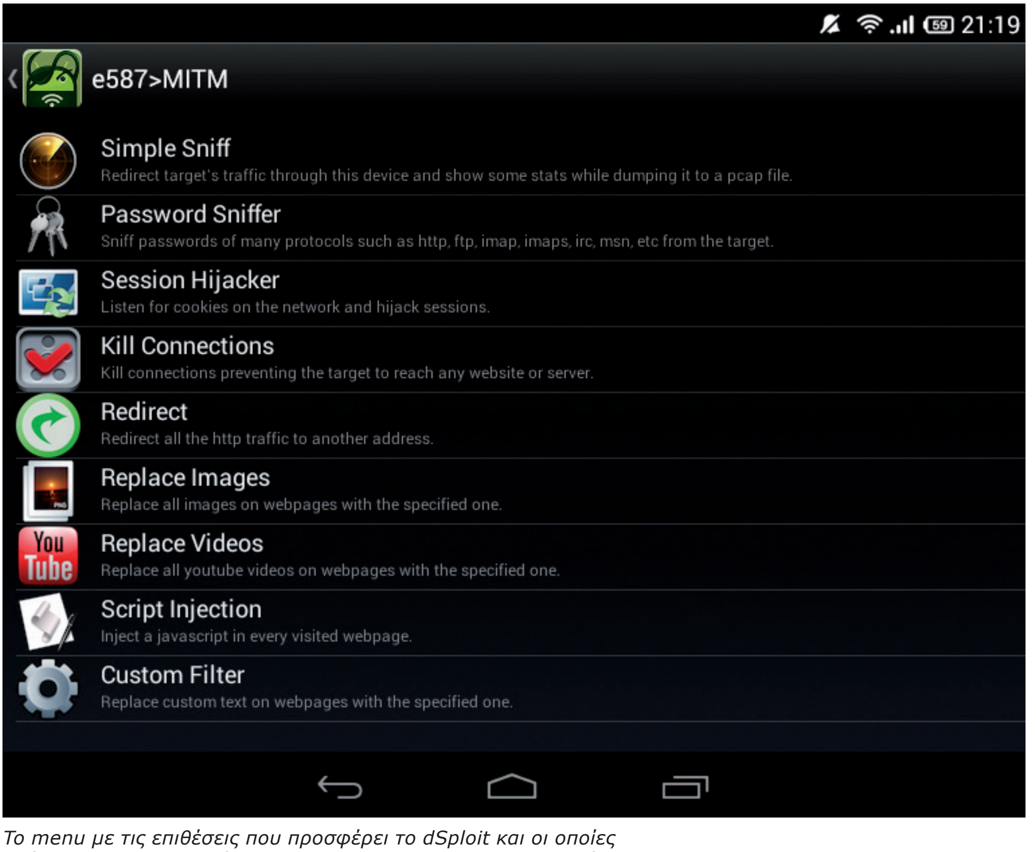
MiTM (Man-in-The-Middle). Εδώ μιλάμε πλέον για μια ολόκληρη κατηγορία επιθέσεων. Όπως γνωρίζετε, οι επιθέσεις αυτού του είδους προβλέπουν την κρυφή και δόλια "παρεμβολή" του δικού μας συστήματος μεταξύ δύο άλλων. Με αυτόν τον τρόπο μπορούμε να υποκλέψουμε όλα τα διακινούμενα δεδομένα. Ας δούμε όπως ποιες συγκεκριμένες επιθέσεις προσφέρει το dSploit.

- **Simple Sniffing.** Το simple sniffing αποτελεί την πιο απλή επίθεση τύπου Man-in-The-Middle. Αυτό που κάνει είναι να ανακατευθύνει στο δικό μας σύστημα όλα τα πακέτα που διακινούνται μεταξύ των δύο ξένων συστημάτων. Το σύνολο αυτών των πακέτων αποθηκεύεται σε ένα αρχείο PCAP, το οποίο μπορούμε να αναλύσουμε με προγράμματα όπως το Wireshark.
- **Password Sniffer.** Αρκετές φορές η πληροφορία που ζητάμε διακαώς είναι κάποιο password — όλα τα υπόλοιπα είναι περιττά ;) Η λειτουργία του password sniffer, λοιπόν, είναι παρόμοια με εκείνη του simple sniffing, με τη διαφορά ότι πραγματοποιείται και μια ανάλυση των δεδομένων, με στόχο την εξαγωγή των passwords.
- **Session Hijacker.** Με αυτή την επίθεση υποκλέπτουμε και πάλι τα διακινούμενα δεδομένα, μόνο που το dSploit δεν αναζητά κάποιο password αλλά τα ενεργά cookies! Με τη βοήθεια αυτών, το dSploit μπορεί να μας "εισάγει" στο session που είχε ξεκινήσει ο χρήστης του συστήματος-στόχου.
- **Kill Connections.** Επί της ουσίας, αυτή η λειτουργία πραγματοποιεί μια επίθεση Denial of Service (DoS): Μπλοκάρει όλα τα πακέτα κι εμποδίζει πλήρως την επικοινωνία του στόχου με το υπόλοιπο δίκτυο. Μεταξύ άλλων, με αυτή τη λειτουργία μπορούμε να ξεφορτωθούμε και τους ενοχλητικούς τύπους που ενδέχεται να έχουν συνδεθεί στο ίδιο ασύρματο δίκτυο με εμάς και οι οποίοι εξαντλούν το διαθέσιμο bandwidth ;)
- **Redirect.** Με αυτή τη λειτουργία μπορούμε να ανακατευθύνουμε όλα τα δεδομένα που ανταλλάσσει το σύστημα-στόχος μέσω HTTP, σε κάποια διεύθυνση της επιλογής μας.
- **Replace Images/Replace Videos.** Αυτή η λειτουργία είναι χρήσιμη και σαν φάρσα :D Εδώ, αντί να ανακατευθύνουμε όλα πακέτα δεδομένων, ανακατευθύνουμε μόνο τα αιτήματα (http requests) για εικόνες ή video. Με αυτόν τον τρόπο μπορούμε να αντικαταστήσουμε τις εικόνες και τα βίντεο που θα έβλεπε υπό φυσιολογικές συνθήκες ο χρήστης του συστήματος-στόχου, με δικές μας εικόνες και βίντεο ή και με παραποιημένες εκδοχές των πρωτότυπων.
- **Script Injection.** Αυτή είναι μια από τις πιο χρήσιμες επιθέσεις, αφού μάς επιτρέπει να γράφουμε κώδικα σε JavaScript και να τον προσθέτουμε στον κώδικα των ιστοσελίδων που βλέπει ο χρήστης του συστήματος-στόχου. Έτσι, ο κώδικάς μας εκτελείται από τον browser του θύματος κανονικότατα και με τη σύνεση του χρήστη!
- **Custom Filter.** Για το τέλος αφήσαμε μια απλή αλλά ύπουλη επίθεση. Πρόκειται για την αλλοίωση ενός τμήματος των πακέτων που λαμβάνει τα σύστημα-στόχος, με στόχο την εξαπάτηση του χρήστη. Για παράδειγμα, μπορούμε να αντικαταστήσουμε τα μηνύματα που βλέπει το θύμα σε κάποια σελίδα, με κάποια που έχουμε συντάξει εμείς οι ίδιοι. Με αυτόν τον τρόπο μπορούμε να προβάλλουμε ψευδή και παραπλανητικά δεδομένα ή ακόμα και να προτρέψουμε το θύμα σε κάποια πράξη που θα ωφελήσει εμάς, αλλά όχι και το ίδιο!

Αντί επιλόγου

Μετά από όσα είπαμε είναι φανερό ότι dSploit αποτελεί ένα άριστο εργαλείο για τον έλεγχο της ασφάλειας του συστήματός μας ή και άλλων, που βρίσκονται στο ίδιο δίκτυο με εμάς. Φυσικά, είναι περιττό να πούμε ότι ένα τέτοιο εργαλείο πρέπει να χρησιμοποιείται με σύνεση! Θα ήταν φρόνιμο να το "στρέφουμε" μόνο προς το δικό μας σύστημα. Όταν θέλουμε να το χρησιμοποιήσουμε σε ξένα συστήματα ή και σε ολόκληρα δίκτυα, θα πρέπει προηγουμένως να έχουμε ζητήσει την άδεια των ιδιοκτητών/χρηστών.

Κάπου εδώ τελειώνει το πρώτο μέρος της σειράς. Κάποιοι ενδέχεται να παραπονεθούν ότι αναλύσαμε μόνο ένα πρόγραμμα και άρα δεν είπαμε και πολλά. Τα πράγματα όμως δεν είναι έτσι. Οι λειτουργίες που παρουσιάσαμε μπορούν να χρησιμοποιηθούν σε δεκάδες είδη επιθέσεων, ενώ οι περισσότερες υλοποιούνται από το dSploit με υποδειγματικό τρόπο. Τώρα βέβαια μπορεί κάποιοι να προβληματιστούν: Εφόσον το dSploit είναι τόσο καλό, τι θα δούμε στο επόμενο άρθρο; Ε λοιπόν, μείνετε συντονισμένοι γιατί ακολουθούν φοβερά και τρομερά πράγματα :D

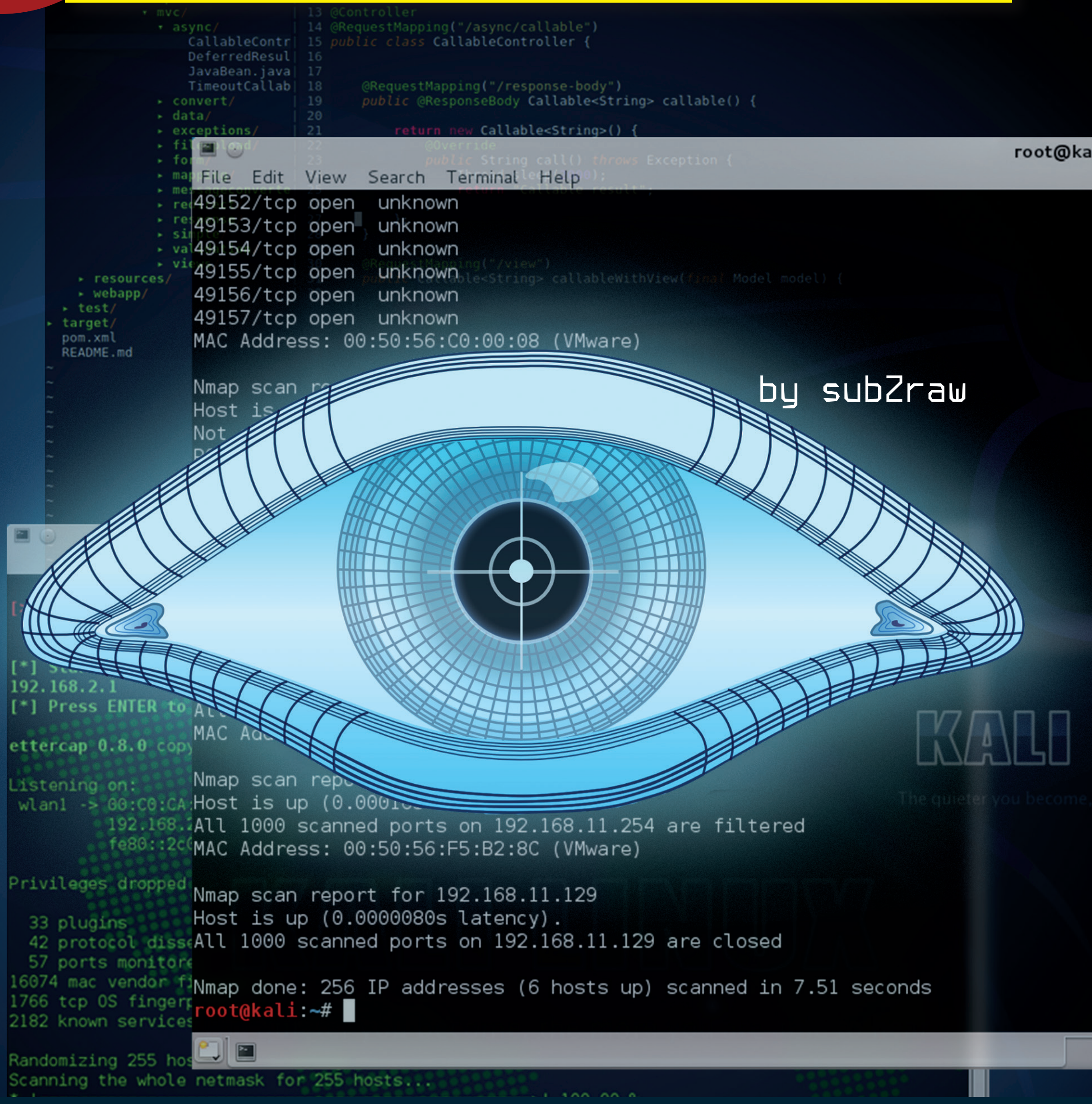


Το menu με τις επιθέσεις που προσφέρει το dSploit και οι οποίες ανήκουν στην κατηγορία Man-in-The-Middle. Όπως αντιλαμβάνεστε, πρόκειται για επιθέσεις που θα ήταν χρονοβόρο και δύσκολο να τις "στήσουμε" χειροκίνητα!



Είμαστε κοινωνικοί — ειδικά στον online κόσμο.
Είμαστε αστείοι, ευφυείς και φινετσάτοι — ειδικά στον online κόσμο.
Λέγεται ότι έχουμε καβαλήσει το καλάμι — τόσο στον online, όσο και στον offline κόσμο.
Όπως και να 'χει, το διαχειριζόμαστε γενναία.
Περάστε από τα στέκια μας να τα πούμε — ή να μας την πείτε.
twitter.com/deltaHacker
facebook.com/deltaHacker

Skill: Beginner
Tags: nmap, port scanning, port state, reverse DNS, ping scan, ping sweep, TCP, UDP, services



by subZraw

Το υπέροχο nmap, από την αρχή

Το nmap δικαιολογημένα συγκαταλέγεται στα πλέον αγαπητά εργαλεία των pen testers αλλά και των network administrators. Ελάτε να γνωρίσουμε το πολύτιμο αυτό εργαλείο ξεκινώντας από τα βασικά, αλλά φωτίζοντας και μερικές από τις όχι και τόσο γνωστές του όψεις.

Το nmap (Network Mapper) είναι ένα δωρεάν εργαλείο ανοικτού λογισμικού με βασική αποστολή την ανακάλυψη μηχανημάτων (hosts) και υπηρεσιών (services) σε ένα τοπικό δίκτυο ή στο Internet. Για να πετυχαίνει το σκοπό του αποστέλλει στους στόχους, δηλαδή στα μηχανήματα που ελέγχει, ειδικά διαμορφωμένα δικτυακά πακέτα με πρωτότυπους τρόπους, κι έπειτα αναλύει τις απαντήσεις που λαμβάνει. Από την ανάλυση αυτή το nmap είναι σε θέση να εντοπίζει:

- τα ενεργά hosts από το σύνολο εκείνων που ελέγχει
- τα ανοικτά ports κάθε host (το τι ακριβώς είναι ένα port μπορείτε να μάθετε από το άρθρο του τεύχους 018, http://deltahacker.gr/?p=8393)
- το λειτουργικό σύστημα κάθε host
- την έκδοση κάθε λειτουργικού
- τις όποιες δικτυακές υπηρεσίες προσφέρει κάθε host
- τις εκδόσεις των υπηρεσιών αυτών
- τα όποια firewalls υπάρχουν στο δίκτυο.

Επιπρόσθετα, χάρη στη μηχανή scripting που ενσωματώνει αλλά και στην πληθώρα των έτοιμων scripts που διατίθενται ελεύθερα γι' αυτό, το nmap έχει τη δυνατότητα να εντοπίζει αδυναμίες (vulnerabilities), backdoors ή malware, να εξαπολύει επιθέσεις denial of service ή brute force, να εκμεταλλεύεται γνωστά bugs σε υπηρεσίες κ.ο.κ. Στο σημείο αυτό πάντως αξίζει να σημειωθεί ότι το nmap δεν είναι —ούτε φιλοδοξεί να γίνει— μια πλήρης πλατφόρμα exploitation όπως, π.χ., είναι το Metasploit.

Το nmap αρχικά διατίθετο μόνο για Linux. Σήμερα παρέχονται binaries για πολλά άλλα Unix-like OSes, για το OS X αλλά και για τα Windows. Αν και το nmap λειτουργεί από τη γραμμή εντολών συχνά συνοδεύεται κι από το Zenmap, ένα εύχρηστο front-end για το περιβάλλον γραφικών.

Σε πολύ λίγο θα γνωρίσουμε το nmap από κοντά, μέσα από μια σειρά παραδειγμάτων χρήσης και δουλεύοντας από την πλατφόρμα του Kali Linux. Το Kali, ως διανομή Linux που προσανατολίζεται στο pen-testing, αμέσως μετά τη βασική του εγκατάσταση παρέχει στο χρήστη τόσο το nmap όσο και μια πληθώρα από επίσημα scripts. Αν δεν έχετε το Kali εύκαιρο προτείνουμε να το κατεβάσετε και να το εγκαταστήσετε τώρα, π.χ., σ' ένα VM (http://kali.org). Μαζί με το Kali φροντίστε να έχετε κι άλλο ένα ή δύο VMs με ενεργές ή/και ευπαθείς υπηρεσίες — και κατά νου έχουμε το Metasploitable (http://bit.ly/getmetasploitable2). Γενικά, επειδή δεν προτείνεται να χρησιμοποιούμε το nmap σε hosts χωρίς πρώτα να έχουμε πάρει σχετική άδεια από τους υπευθύνους, είναι προτιμότερο να το γνωρίσουμε στο πλαίσιο ενός εικονικού εργαστηρίου. Στο deltaCast s01e06 μπορείτε να παρακολουθήσετε αναλυτικές οδηγίες για το στήσιμο του δικού σας εργαστηρίου (http://deltahacker.gr/deltacast-s01e06). Υπόψη ότι στο εν λόγω video tutorial επιδεικνύεται η εγκατάσταση του BackTrack, του προγόνου του Kali Linux. Το BackTrack όμως έχει σταματήσει ν' αναπτύσσεται, οπότε οδηγίες για την εγκατάσταση και ρύθμιση του Kali υπάρχουν στο site του περιοδικού και συγκεκριμένα στο http://deltahacker.gr/?p=9070.

Σημείωση. Στο Kali Linux εξ ορισμού δουλεύουμε από το λογαριασμό του διαχειριστή συστήματος, μ' άλλα λόγια ως root. Αν δοκιμάσετε τα παραδείγματά μας από άλλη διανομή Linux ή από άλλο λειτουργικό σύστημα, έχετε υπόψη σας ότι ορισμένες φορές θα απαιτούνται δικαιώματα υπερχρήστη. Το nmap θα σας ενημερώνει σχετικά.

Καθορισμός στόχων, αξιολόγηση αποτελεσμάτων

Η γενική σύνταξη μιας εντολής σάρωσης (scan) με το nmap έχει ως εξής:

```
nmap [είδος σάρωσης] [επιλογές & παράμετροι] <στόχος ή στόχοι>
```

Ξεκινάμε από μια απλούστατη περίπτωση: τη σάρωση ενός μόνο μηχανήματος του τοπικού δικτύου, με διεύθυνση IP την 192.168.85.111. Στο Kali μας, ανοίγουμε ένα παράθυρο τερματικού και πληκτρολογούμε:

```
root@kali:~# nmap 192.168.85.111
Starting Nmap 6.46 ( http://nmap.org ) at 2014-08-22 23:29 EEST
Nmap scan report for 192.168.85.111
Host is up (0.00018s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
```

```
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:EC:48:E4 (Cadmus Computer Systems)
Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds
root@kali:~#
```

(Τονισμένο είναι ό,τι γράφουμε εμείς, όλα τ' άλλα είναι αποτελέσματα που παίρνουμε στο τερματικό.) Δεν καθορίσαμε το είδος της σάρωσης, ούτε κάναμε κάποια συγκεκριμένη επιλογή. Μολαταύτα, σε λιγότερο από ένα δευτερόλεπτο το nmap επέστρεψε:

- τις ανοικτές θύρες (ports) του στόχου
- την κατάσταση (state) κάθε port
- το όνομα της υπηρεσίας που εξ ορισμού χρησιμοποιεί ένα συγκεκριμένο port
- τη διεύθυνση MAC του δικτυακού interface του στόχου.

Για το nmap, οι θύρες βρίσκονται σε μία από τις ακόλουθες τέσσερις καταστάσεις:

Open. Υπάρχει ενεργή υπηρεσία που χρησιμοποιεί τη θύρα.

Closed. Δεν υπάρχει υπηρεσία που να χρησιμοποιεί τη θύρα, ωστόσο αυτό είναι πιθανό ν' αλλάξει ανά πάσα στιγμή.

Filtered. Κάποιο firewall ή κάτι άλλο εμποδίζει το nmap από το να συμπεράνει αν η θύρα είναι open ή closed.

Unfiltered. Υπάρχει κάποια ανταπόκριση στους ελέγχους του nmap, εξακολουθεί ωστόσο να 'ναι αδύνατος ο χαρακτηρισμός της θύρας ως open ή ως closed.

Το nmap είναι επίσης πιθανό να επιστρέψει τους συνδυασμούς καταστάσεων open|filtered ή closed|filtered, όταν αδυνατεί να συμπεράνει σε ποια από τις δύο καταστάσεις είναι η εκάστοτε θύρα.

Στο παράδειγμα που μόλις δώσαμε σκανάραμε *ένα* μόνο μηχάνημα του τοπικού δικτύου. Ας πάμε τώρα στο άλλο άκρο, όπου σκανάρουμε *όλα* τα μηχανήματα του τοπικού δικτύου. Η σύνταξη του nmap παραμένει απλή — κι αν αυτό το "/24" σας παραξενέψει, είναι επειδή δεν έχετε διαβάσει ακόμα το άρθρο στο http://deltahacker.gr/hownetsworkpart2b.

```
root@kali:~# nmap 192.168.85.0/24
Starting Nmap 6.46 ( http://nmap.org ) at 2014-08-23 10:05 EEST
Nmap scan report for localrouter.parabing.local (192.168.85.1)
Host is up (0.00033s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
13/tcp  open  daytime
22/tcp  open  ssh
37/tcp  open  time
53/tcp  open  domain
113/tcp open  ident
MAC Address: 08:00:27:05:A3:2A (Cadmus Computer Systems)

Nmap scan report for win7host.parabing.local (192.168.85.10)
Host is up (0.00025s latency).
Not shown: 992 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
...
10243/tcp open  unknown
MAC Address: 02:00:4C:4F:4F:50 (Unknown)

Nmap scan report for 192.168.85.111
Host is up (0.00019s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
...
8180/tcp open  unknown
MAC Address: 08:00:27:EC:48:E4 (Cadmus Computer Systems)

Nmap scan report for JoePC.parabing.local (192.168.85.112)
Host is up (0.00020s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
```

```
135/tcp   open  msrpc
...
49158/tcp open  unknown
MAC Address: 08:00:27:79:37:C5 (Cadmus Computer Systems)

Nmap scan report for secdesk.parabing.local (192.168.85.125)
Host is up (0.00019s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
...
1027/tcp open  IIS
MAC Address: 08:00:27:67:0E:3D (Cadmus Computer Systems)

Nmap scan report for trusty.parabing.local (192.168.85.141)
Host is up (0.00022s latency).
All 1000 scanned ports on trusty.parabing.local (192.168.85.141) are
closed
MAC Address: 08:00:27:59:2F:CB (Cadmus Computer Systems)

Nmap scan report for kali.parabing.local (192.168.85.20)
Host is up (0.000016s latency).
All 1000 scanned ports on kali.parabing.local (192.168.85.20) are closed

Nmap done: 256 IP addresses (7 hosts up) scanned in 23.44 seconds
root@kali:~#
```

Αυτή τη φορά, τα αποτελέσματα που παίρνουμε ίσως μοιάζουν περισσότερα απ' όσα θα μπορούσαμε να διαχειριστούμε. Αλλά δεν είναι έτσι τα πράγματα. Αν λοιπόν παρατηρήσουμε με την ησυχία μας την έξοδο του nmap, εύκολα μπορούμε να συμπεράνουμε τα ακόλουθα:

- Ελέγχθηκαν 256 διευθύνσεις IP και βρέθηκαν 7 ενεργά hosts.
- Για τα ενεργά hosts το nmap πραγματοποίησε σχετικά DNS queries, ώστε να μάθει τα μνημονικά ονόματά τους. Για την ακρίβεια, αυτό που έκανε το nmap είναι τα λεγόμενα reverse DNS lookups ή αλλιώς reverse DNS resolutions (rDNS), προκειμένου να μάθει το domain name που αντιστοιχεί στη διεύθυνση IP κάθε ενεργού host.

- Το nmap έμαθε τα domain names των 6 από τα 7 ενεργά hosts (βλ., π.χ., localrouter.parabing.local, win7host.parabing.local κ.ο.κ.).
- Για κάποια hosts, όπως αυτό το JoePC.parabing.local (192.168.85.112), το nmap βρήκε ανοικτά ports αλλά δεν αναγνώρισε τις υπηρεσίες πίσω τους (unknown). Είναι πάντως σε θέση να τα καταφέρνει και καλύτερα. Θα δούμε σε λίγο πώς.
- Τα 5 από τα 7 ενεργά hosts έχουν διάφορα ανοικτά ports. Εξαίρεση αποτελούν τα trusty.parabing.local (192.168.85.141) και kali.parabing.local (192.168.85.20), τα οποία μοιάζουν να μην έχουν ούτε ένα port ανοικτό.

Βλέπουμε ότι σε κάθε host το nmap ελέγχει 1000 στο πλήθος ports. Αυτή είναι η προκαθορισμένη συμπεριφορά. Αν του ζητήσουμε να ελέγξει περισσότερα ports —και θα δούμε αργότερα πώς του το ζητάμε— ίσως αποδειχθεί ότι hosts σαν το kali.parabing.local δεν είναι και τόσο "stealth" όσο αρχικά δείχνουν.

Ας σταθούμε λίγο και στα domain names. Κάποια εξ αυτών, όπως το localrouter.parabing.local, φανερώνουν το *είδος* του αντίστοιχου host. Αυτό το localrouter.parabing.local, για παράδειγμα, μας λέει ότι το 192.168.85.1 μάλλον είναι ο router του τοπικού δικτύου στο οποίο τώρα βρισκόμαστε και κάνουμε τις δοκιμές μας. Μπορεί πράγματι να 'ναι ο router, μπορεί όμως κι όχι. Υπάρχουν διάφοροι τρόποι για να βρούμε τον router κι ένας απ' αυτούς είναι με τη βοήθεια του ίδιου του nmap:

```
root@kali:~# nmap --iflist
Starting Nmap 6.46 ( http://nmap.org ) at 2014-08-23 12:19 EEST
************************INTERFACES************************
...
**************************ROUTES**************************
DST/MASK                      DEV  METRIC GATEWAY
192.168.85.0/24               eth0 0
0.0.0.0/0                     eth0 0      192.168.85.1
::1/128                       lo   0
fe80::a00:27ff:fe8a:a336/128  lo   0
fe80::/64                     eth0 256
ff00::/8                      eth0 256
root@kali:~#
```

Με μια ματιά στις στήλες DST/MASK και GATEWAY, επαληθεύουμε ότι ο 192.168.85.1 είναι πράγματι ο router του τοπικού δικτύου.

Το domain name μερικές φορές φανερώνει πολλά και για το λειτουργικό που τρέχει ο host. Παράδειγμα: Το win7host.parabing.local μάς κάνει να πιστεύουμε ότι το μηχάνημα με IP το 192.168.85.10, τρέχει Windows 7. Επίσης, αυτό το trusty.parabing.local μάς υποψιάζει ότι το 192.168.85.141 τρέχει Ubuntu Linux 14.04 (κωδική ονομασία Trusty Tahr). Υπογραμμίζουμε πάντως ότι με βάση το domain name και μόνο, ασφαλή συμπεράσματα για το λειτουργικό του host ούτε μπορούμε ούτε δικαιούμαστε να βγάζουμε. Ευτυχώς, το nmap είναι σε θέση να μας βοηθήσει και σ' αυτόν τον

τομέα. Περισσότερα επ' αυτού θα δούμε στη συνέχεια του άρθρου.

Μέχρι στιγμής δείξαμε πώς σκανάρουμε ένα host και πώς ένα ολόκληρο δίκτυο. Αλλά το nmap είναι πολύ πιο ευέλικτο, όσον αφορά στον προσδιορισμό στόχων. Το τι εννοούμε φαίνεται στα παραδείγματα που ακολουθούν.

- **Σάρωση συγκεκριμένων hosts,** τοπικά και στο Intentet:

  ```
  root@kali:~# nmap 192.168.85.1 192.168.85.111 192.168.85.141
  ```

  Φυσικά, αν για κάποιο host γνωρίζουμε το domain name του, μπορούμε να δίνουμε και κάτι τέτοιο:

  ```
  root@kali:~# nmap localrouter.parabing.local 192.168.85.111 trusty.
  parabing.local
  ```

  Όπως έχουμε ήδη αναφέρει, το nmap δεν έχει κανένα απολύτως πρόβλημα να σκανάρει hosts στο Internet:

  ```
  root@kali:~# nmap scanme.nmap.org
  Starting Nmap 6.46 ( http://nmap.org ) at 2014-08-23 13:41 EEST
  Nmap scan report for scanme.nmap.org (74.207.244.221)
  Host is up (0.22s latency).
  Not shown: 997 closed ports
  PORT     STATE SERVICE
  22/tcp   open  ssh
  80/tcp   open  http
  9929/tcp open  nping-echo
  Nmap done: 1 IP address (1 host up) scanned in 3.96 seconds
  root@kali:~#
  ```

- Αν οι υπό σάρωση hosts έχουν IPs που διαφέρουν μόνον ως προς **το τελευταίο octet**, τότε μπορούμε να δίνουμε:

  ```
  root@kali:~# nmap 192.168.85.1,111,141
  ```

- **Εναλλακτικός τρόπος** σάρωσης subnet:

  ```
  root@kali:~# nmap 192.168.85.*
  ```

Το ίδιο αποτέλεσμα είχαμε πετύχει προηγουμένως, δίνοντας "nmap 192.168.85.0/24".

- **Σάρωση "συνεχούς" υποσυνόλου** ενός subnet (IP address range):

  ```
  root@kali:~# nmap 192.168.85.100-150
  ```

- Σάρωση hosts **από λίστα σε αρχείο**:

  ```
  root@kali:~# nmap -iL hosts.list
  ```

  Το hosts.list είναι ένα αρχείο απλού κειμένου (εννοείται ότι το ονομάζουμε όπως θέλουμε), το οποίο σε κάθε γραμμή περιέχει τη διεύθυνση IP ή το

domain name ενός host. Εναλλακτικά, σε κάποιες ή σε όλες από τις γραμμές του hosts.list επιτρέπεται να ορίζονται network blocks (π.χ., με τη μορφή CIDR) ή IP address ranges. Μέσα στο hosts.list μπορούμε να έχουμε και γραμμές με σχόλια. Κάθε τέτοια γραμμή ξεκινά με το χαρακτήρα # κι εκτείνεται έως το τέλος της.

- **Σάρωση με εξαιρέσεις:**

```
root@kali:~# nmap 192.168.85.5-200 --exclude 192.168.85.30
```

Στο παράδειγμα σαρώνουμε όλα τα μηχανήματα από το 192.168.85.5 έως και το 192.168.85.200, αλλά όχι το 192.168.85.30 (π.χ., επειδή γνωρίζουμε ότι τρέχει κάποιο IDS και δεν θέλουμε να χτυπήσει συναγερμός). Η παράμετρος --exclude μπορεί να δεχθεί μια λίστα από hosts, network blocks ή και ranges, τα οποία χωρίζονται μεταξύ τους με κόμματα. Τα hosts που επιθυμούμε να εξαιρούνται είναι δυνατόν να διαβάζονται από ένα αρχείο, οπότε σ' αυτές τις περιπτώσεις χρησιμοποιούμε την παράμετρο --excludefile:

```
root@kali:~# nmap 192.168.85.5-200 --excludefile hosts.list
```

Για τη σύνταξη του hosts.list ισχύουν όλα όσα αναφέραμε πριν λίγο, όταν συζητούσαμε για τα αρχεία που δίνουμε στην παράμετρο -iL.

- **Συνδυασμοί:**

```
root@kali:~# nmap -sL 192.168.85.1-40 192.168.85.70-245
192.168.85.250 --exclude 192.168.85.130-160
```

- **Τυχαία σάρωση:**

```
root@kali:~# nmap -iR 10
```

Με την παραπάνω εντολή ζητάμε τη σάρωση 10 στο πλήθος *τυχαίων* hosts στο Internet. Γενικά, η παράμετρος -iR δέχεται το πλήθος των τυχαίων διευθύνσεων που θα παραγάγει. Έχετε κατά νου ότι αρκετοί διαχειριστές δεν εκτιμούν τις "αυθόρμητες" σαρώσεις των hosts που έχουν υπό την εποπτεία τους. Δεν αποκλείεται να παραπονεθούν στον ISP σας κι εκείνος με τη σειρά του να παραπονεθεί σ' εσάς. Χρησιμοποιείτε την παράμετρο -iR μόνον όταν ξέρετε πολύ καλά τι πάτε να κάνετε κι έχοντας πλήρη συνείδηση των πιθανών συνεπειών.

Διερεύνηση για ενεργά hosts, υπηρεσίες & λειτουργικά

Μερικές φορές θέλουμε να βρούμε στα γρήγορα όλα τα ενεργά hosts ενός δικτύου ή ενός τμήματος δικτύου ή, τέλος πάντων, μιας λίστας από hosts. Σε τέτοιες περιπτώσεις χρησιμοποιούμε την επιλογή -sn, η οποία λέει στο nmap να μην κάνει port scan αλλά μόνο ένα "ping scan" ή αλλιώς "ping sweep". Παράδειγμα:

```
root@kali:~# nmap -sn 192.168.85.1-254
Starting Nmap 6.46 ( http://nmap.org ) at 2014-08-24 13:03 EEST
Nmap scan report for localrouter.parabing.local (192.168.85.1)
Host is up (0.00058s latency).
```

```
MAC Address: 08:00:27:05:A3:2A (Cadmus Computer Systems)
Nmap scan report for win7host.parabing.local (192.168.85.10)
Host is up (0.00025s latency).
MAC Address: 02:00:4C:4F:4F:50 (Unknown)
Nmap scan report for 192.168.85.111
Host is up (0.0014s latency).
MAC Address: 08:00:27:EC:48:E4 (Cadmus Computer Systems)
Nmap scan report for JoePC.parabing.local (192.168.85.112)
Host is up (0.00095s latency).
MAC Address: 08:00:27:79:37:C5 (Cadmus Computer Systems)
Nmap scan report for secdesk.parabing.local (192.168.85.125)
Host is up (0.00063s latency).
MAC Address: 08:00:27:67:0E:3D (Cadmus Computer Systems)
Nmap scan report for trusty.parabing.local (192.168.85.141)
Host is up (0.00024s latency).
MAC Address: 08:00:27:59:2F:CB (Cadmus Computer Systems)
Nmap scan report for kali.parabing.local (192.168.85.20)
Host is up.
Nmap done: 254 IP addresses (7 hosts up) scanned in 1.84 seconds
root@kali:~#
```

Όπως φαίνεται στ' αποτελέσματα, από τα 254 hosts που θα μπορούσαν να υπάρχουν στο μικρό μας δίκτυο, το nmap εντόπισε 7 ενεργά hosts.

Προηγουμένως, εξάλλου, είδαμε ότι το nmap δεν μπορούσε να είναι σίγουρο για τις υπηρεσίες που έτρεχαν σε κάποια hosts. Επιπρόσθετα, μερικές φορές είναι σημαντικό να γνωρίζουμε όχι μόνο το όνομα μιας υπηρεσίας, αλλά και την έκδοσή της. Ίσως, π.χ., να ξέρουμε ότι η τάδε έκδοση ενός συγκεκριμένου FTP server έχει μια συγκεκριμένη αδυναμία, την οποία ένας attacker θα μπορούσε να εκμεταλλευτεί προκειμένου ν' αποκτήσει μη εξουσιοδοτημένη πρόσβαση στον server. Το nmap έχει τη δυνατότητα συλλογής μιας πληθώρας πληροφοριών για τις υπηρεσίες, αρκεί να του δώσουμε την επιλογή -sV. Ένας τρόπος για να δείτε στην πράξη πώς δουλεύει η -sV, είναι να κάνετε δύο scans στο VM με το Metasploitable (για εμάς είναι το host με IP το 192.168.85.111). Το ένα scan είναι χωρίς την -sV...

```
root@kali:~# nmap -sV 192.168.85.111
```

και το άλλο είναι ίδιο αλλά έχει την επιλογή -sV:

```
root@kali:~# nmap -sV 192.168.85.111
Starting Nmap 6.46 ( http://nmap.org ) at 2014-08-24 16:19 EEST
Nmap scan report for 192.168.85.111
Host is up (0.00071s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         Unreal ircd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:EC:48:E4 (Cadmus Computer Systems)
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.
Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.41 seconds
root@kali:~#
```

Στο δεύτερο scan οι πληροφορίες περί έκδοσης των υπηρεσιών είναι στη νέα στήλη, ονόματι VERSION. Παρατηρήστε επίσης ότι το nmap βρήκε κάτι και για την υπηρεσία πίσω από το port 8180/TCP, η οποία στο πρώτο scan ήταν χαρακτηρισμένη ως "unknown".

Εκτός από υπηρεσίες, το nmap έχει τον τρόπο του να μαθαίνει πληροφορίες για το λειτουργικό που τρέχει ένας host. Η επιλογή γι' αυτή τη δουλειά είναι η -O:

```
root@kali:~# nmap -O 192.168.85.112
Starting Nmap 6.46 ( http://nmap.org ) at 2014-08-24 17:12 EEST
Nmap scan report for JoePC.parabing.local (192.168.85.112)
Host is up (0.00027s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49158/tcp open  unknown
MAC Address: 08:00:27:79:37:C5 (Cadmus Computer Systems)
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_8
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, or
Windows 8
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at http://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.21 seconds
root@kali:~#
```

Σύμφωνα με την ανάλυση του nmap, το 192.168.85.112 τρέχει Windows 7 ή Windows 2008. Όπως κάναμε και προηγουμένως, έτσι και τώρα μπορούμε να συνδυάζουμε επιλογές:

```
root@kali:~# nmap -O -sV 192.168.85.112
Starting Nmap 6.46 ( http://nmap.org ) at 2014-08-24 17:18 EEST
Nmap scan report for JoePC.parabing.local (192.168.85.112)
Host is up (0.00030s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE     VERSION
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
5357/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc       Microsoft Windows RPC
49153/tcp open  msrpc       Microsoft Windows RPC
49154/tcp open  msrpc       Microsoft Windows RPC
49155/tcp open  msrpc       Microsoft Windows RPC
49156/tcp open  msrpc       Microsoft Windows RPC
49158/tcp open  msrpc       Microsoft Windows RPC
MAC Address: 08:00:27:79:37:C5 (Cadmus Computer Systems)
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_8
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, or
Windows 8
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
OS and Service detection performed. Please report any incorrect results
at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 56.66 seconds
root@kali:~#
```

Καθορισμός θυρών και πρωτοκόλου

Όταν σκανάρουμε ένα host, εξ ορισμού το nmap ελέγχει τα 1000 πιο συνηθισμένα TCP ports. Προφανώς, ένα host είναι πιθανό να 'χει κάποιο port ανοικτό αλλά αυτό να μη συγκαταλέγεται στα 1000 πιο συνηθισμένα. Δείτε αυτό το παράδειγμα:

```
root@kali:~# nmap 192.168.85.20
Starting Nmap 6.46 ( http://nmap.org ) at 2014-08-24 18:55 EEST
Nmap scan report for kali.parabing.local (192.168.85.20)
Host is up (0.000013s latency).
All 1000 scanned ports on kali.parabing.local (192.168.85.20) are closed
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
root@kali:~#
```

Αν το 192.168.85.20 έχει κάποιο port ανοικτό, αυτό δεν είναι ανάμεσα στα 1000 πιο συνηθισμένα. Με την επιλογή -p μπορούμε να πούμε στο nmap ποια ports να ελέγξει. Μιας και τώρα πειραματιζόμαστε με ασφάλεια εντός του εικονικού μας εργαστηρίου, ας ακολουθήσουμε μια κάπως χοντροκομμένη τακτική κι ας ζητήσουμε από το nmap να ελέγξει *όλα* τα TCP ports του στόχου:

```
root@kali:~# nmap -p 1-65535 192.168.85.20
Starting Nmap 6.46 ( http://nmap.org ) at 2014-08-24 18:59 EEST
Nmap scan report for kali.parabing.local (192.168.85.20)
Host is up (0.000017s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE
12222/tcp open  unknown
Nmap done: 1 IP address (1 host up) scanned in 3.25 seconds
root@kali:~#
```

Να λοιπόν που ο στόχος μας έχει ένα TCP port ανοικτό: το 12222. Η υπηρεσία πίσω απ' αυτό δείχνει άγνωστη, όμως δεν υπάρχει κανένας λόγος να κάνουμε υποθέσεις:

```
root@kali:~# nmap -p 12222 -sV 192.168.85.20
Starting Nmap 6.46 ( http://nmap.org ) at 2014-08-24 19:06 EEST
Nmap scan report for kali.parabing.local (192.168.85.20)
Host is up (0.000081s latency).
PORT      STATE SERVICE VERSION
12222/tcp open  ssh     OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
root@kali:~#
```

Μάλιστα! Ο ιδιοκτήτης του 192.168.85.20 έχει απλά αλλάξει την προκαθορισμένη θύρα που χρησιμοποιεί η υπηρεσία OpenSSH (είναι η 22/TCP), προφανώς για λόγους ασφαλείας. Αυτή η τακτική συνηθίζεται στους servers, στο πλαίσιο των μέτρων ασφαλείας κατά "αφελών" scipts που ψάχνουν για δημοφιλείς υπηρεσίες στα τυφλά. Όπως όμως αποδεικνύει το απλό παράδειγμά μας, κάποιος που είναι αποφασισμένος να μάθει αν τρέχουμε μια συγκεκριμένη υπηρεσία ή όχι, χάρη στο nmap είναι πολύ εύκολο να κάνει τους ελέγχους του.

Στο σημείο αυτό σίγουρα φαντάζεστε ότι η επιλογή -p είναι αρκετά πιο ευέλικτη απ' όσο φανερώνουν τα δύο προηγούμενα παραδείγματα. Πράγματι, έτσι είναι. Ας πούμε, π.χ., ότι βαριόμαστε λίγο και θέλουμε να βρούμε —έτσι, για πλάκα— μηχανήματα στο Internet τα οποία τρέχουν κάποιον web server ή έχουν την υπηρεσία OpenSSH ενεργοποιημένη. Υποθέτοντας ότι χρησιμοποιούνται οι προκαθορισμένες θύρες, η 80/TCP και η 22/TCP αντίστοιχα, ας δοκιμάσουμε 500 hosts *εντελώς* στην τύχη:

```
root@kali:~# nmap -v -Pn -p 22,80 --open -oN random.hosts -iR 500
Starting Nmap 6.46 ( http://nmap.org ) at 2014-08-24 19:32 EEST
Initiating Parallel DNS resolution of 500 hosts. at 19:32
Completed Parallel DNS resolution of 500 hosts. at 19:32, 19.19s elapsed
Initiating SYN Stealth Scan at 19:32
Scanning 500 hosts [2 ports/host]
Discovered open port 80/tcp on p.q.r.s
Discovered open port 80/tcp on x.y.z.t
...
Discovered open port 22/tcp on a.b.c.d
Discovered open port 80/tcp on i.j.k.l
...
Discovered open port 22/tcp on s.t.u.v
...
Completed SYN Stealth Scan at 19:33, 37.92s elapsed (1000 total ports)
Nmap scan report for real-domain-name.hidden.net (e.f.g.h)
Host is up (0.41s latency).
Not shown: 1 filtered port
PORT   STATE SERVICE
```

```
80/tcp open  http
...
root@kali:~#
```

Στην παραπάνω εντολή υπάρχουν τρεις επιλογές του nmap για τις οποίες δεν έχουμε ακόμα συζητήσει. Κατ' αρχάς, η -v αυξάνει το πλήθος των πληροφοριών που εμφανίζει το nmap στο τερματικό καθώς εργάζεται. Κάποιες σαρώσεις παίρνουν αρκετή ώρα για να ολοκληρωθούν κι όταν βλέπουμε "δράση" στην οθόνη βεβαιωνόμαστε ότι όλα προχωράνε κι ο χρόνος μας δεν πηγαίνει (εντελώς) χαμένος. Ενδιαφέρουσα είναι η παράμετρος -Pn, η οποία ζητά από το nmap να *μη* χρησιμοποιεί ping scans προκειμένου να εντοπίζει ενεργά hosts. Αντίθετα, με την -Pn το nmap θεωρεί ότι όλοι οι στόχοι του είναι ενεργοί και συνεχίζει με τους όποιους άλλους ελέγχους του έχουμε ζητήσει να επιτελέσει. Γιατί όμως να θέλουμε την επιλογή -Pn; Πολύ απλά διότι αρκετοί servers, ειδικά στο Internet, προστατεύονται από firewalls τα οποία είναι ρυθμισμένα ώστε να αγνοούν εντελώς τα pings. Ας δούμε τώρα και την επιλογή --open. Η συμπερίληψή της σε μια σάρωση διαμορφώνει τα αποτελέσματα που παίρνουμε, ώστε να περιλαμβάνουν hosts που έχουν *τουλάχιστον* ένα open, open|filtered ή unfiltered port. Μ' άλλα λόγια, όταν υπάρχει η επιλογή --open τότε δεν βλέπουμε hosts τα οποία έχουν *μόνο* closed, filtered ή closed|filtered ports. Με την επιλογή -oN, εξάλλου, η οποία ακολουθείται από ένα όνομα αρχείου, ζητάμε από το nmap να αποθηκεύσει τα αποτελέσματα σε ένα αρχείο απλού κειμένου. Μιας και πριν λίγο ξεκινήσαμε τη σάρωση 500 στο πλήθος τυχαίων hosts, είναι αναμενόμενο ότι τ' αποτελέσματα του nmap θα γεμίσουν το τερματικό και γι' αυτό είναι καλό να τ' αποθηκεύσουμε και σ' ένα αρχείο. Εκτός από την -oN, υπάρχουν τρεις άλλες επιλογές για την αποθήκευση αποτελεσμάτων. Από αυτές ιδιαίτερα χρήσιμη είναι η -oX, η οποία αποθηκεύει σε αρχεία μορφής XML. Τα αρχεία του είδους αναγνωρίζουν κι ανοίγουν διάφορες εφαρμογές, μεταξύ αυτών και το front-end γραφικών Zenmap.

Κατά τη διάρκεια των πειραματισμών μας, μεταξύ των 500 hosts που ελέγξαμε βρήκαμε κάποιους που έτρεχαν web servers, άλλους που έτρεχαν SSH servers, καθώς και έναν που έτρεχε και τις δύο υπηρεσίες ταυτόχρονα.

Λίγο πριν ολοκληρώσουμε την εισαγωγή μας στο nmap, ας δούμε μερικές ακόμα όψεις του που αφορούν στην επιλογή ports για σάρωση. Στα έως τώρα παραδείγματά μας το nmap ήλεγχε TCP ports. Έχει όμως την ικανότητα να ελέγχει και UDP ports, με την επιλογή -sU. Δείτε:

```
root@kali:~# nmap -sU 192.168.85.1
Nmap scan report for localrouter.parabing.local (192.168.85.1)
Host is up (0.00040s latency).
Not shown: 996 closed ports
PORT     STATE          SERVICE   VERSION
53/udp   open           domain    dnsmasq 2.65
```

```
67/udp   open|filtered dhcps
514/udp  open|filtered syslog
4500/udp open|filtered nat-t-ike
MAC Address: 08:00:27:05:A3:2A (Cadmus Computer Systems)
Device type: firewall|general purpose
Running: Genua OpenBSD 4.X, OpenBSD 3.X|4.X|5.X
OS CPE: cpe:/o:genua:openbsd:4 cpe:/o:openbsd:openbsd:3.4 cpe:/
o:openbsd:openbsd:4
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
OS and Service detection performed. Please report any incorrect results
at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 159.60 seconds
root@kali:~#
```

Με μία σάρωση έχουμε τη δυνατότητα να ελέγχουμε TCP αλλά και UDP ports, ταυτόχρονα. Αν, π.χ., θέλουμε να ψάξουμε στα γρήγορα το τοπικό δίκτυο για μηχανήματα που μοιράζουν αρχεία κατά SMB/CIFS, δέχονται συνδέσεις SSH ή παρέχουν υπηρεσίες DNS, ένας τρόπος για να τα εντοπίσουμε είναι με τη βοήθεια του nmap:

```
root@kali:~# nmap -sS -sU -p T:22,137-139,389,445,901,U:53,137-139
--open 192.168.85.*
Starting Nmap 6.46 ( http://nmap.org ) at 2014-08-25 00:07 EEST
Nmap scan report for localrouter.parabing.local (192.168.85.1)
Host is up (0.0073s latency).
Not shown: 9 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
53/udp open  domain
MAC Address: 08:00:27:05:A3:2A (Cadmus Computer Systems)

Nmap scan report for win7host.parabing.local (192.168.85.10)
Host is up (0.00042s latency).
Not shown: 5 filtered ports
PORT     STATE         SERVICE
139/tcp open           netbios-ssn
```

```
445/tcp open          microsoft-ds
53/udp  open|filtered domain
137/udp open          netbios-ns
138/udp open|filtered netbios-dgm
139/udp open|filtered netbios-ssn
MAC Address: 02:00:4C:4F:4F:50 (Unknown)
Nmap scan report for 192.168.85.111
Host is up (0.0012s latency).
Not shown: 5 closed ports
PORT    STATE         SERVICE
22/tcp  open          ssh
139/tcp open          netbios-ssn
445/tcp open          microsoft-ds
53/udp  open          domain
137/udp open          netbios-ns
138/udp open|filtered netbios-dgm
MAC Address: 08:00:27:EC:48:E4 (Cadmus Computer Systems)

Nmap scan report for JoePC.parabing.local (192.168.85.112)
Host is up (0.0011s latency).
Not shown: 7 closed ports
PORT    STATE         SERVICE
139/tcp open          netbios-ssn
445/tcp open          microsoft-ds
137/udp open          netbios-ns
138/udp open|filtered netbios-dgm
MAC Address: 08:00:27:79:37:C5 (Cadmus Computer Systems)

Nmap scan report for secdesk.parabing.local (192.168.85.125)
Host is up (0.00040s latency).
Not shown: 7 closed ports
PORT    STATE         SERVICE
139/tcp open          netbios-ssn
445/tcp open          microsoft-ds
137/udp open          netbios-ns
138/udp open|filtered netbios-dgm
```

```
MAC Address: 08:00:27:67:0E:3D (Cadmus Computer Systems)

Nmap done: 256 IP addresses (7 hosts up) scanned in 6.03 seconds
root@kali:~#
```

Το nmap βρήκε 7 ενεργά hosts. Λόγω όμως της επιλογής --open, παρουσιάζει τα 5 που έχουν ανοικτή τουλάχιστον μία από τις θύρες 22/TCP, 137/TCP, 138/TCP, 139/TCP, 389/TCP, 445/TCP, 901/TCP, 53/UDP, 137/UDP, 138/UDP, 139/UDP. Έχετε κατά νου ότι προκειμένου να πραγματοποιούνται τόσο TCP όσο και UDP scans ταυτόχρονα, στο nmap οφείλουμε να δίνουμε την επιλογή -sU αλλά και να καθορίζουμε το είδος του TCP scan. Όταν το nmap τρέχει από το λογαριασμό του διαχειριστή συστήματος, όπως συμβαίνει με τα παραδείγματά μας, τότε εξ ορισμού πραγματοποιούνται TCP SYN scans. Η σχετική επιλογή για το nmap είναι η -sS και —αν και υπονοείται— όποτε επιθυμούμε να γίνεται *και* UDP scan τότε υποχρεούμαστε να τη δίνουμε στη γραμμή εντολής.

Μία άλλη, ενδιαφέρουσα, επιλογή που αφορά στα ports είναι η --top-ports. Δέχεται ως όρισμα έναν θετικό ακέραιο k, ο οποίος αντιπροσωπεύει τα k πιο δημοφιλή ports ανά πρωτόκολλο (TCP, UDP) που είναι ανοικτά σε servers κι αναφέρονται στο αρχείο nmap-services (/usr/share/nmap/nmap-services). Σημειώστε ότι οι πληροφορίες στο εν λόγω αρχείο έχουν προκύψει μετά από πραγματική έρευνα στο Internet. Παράδειγμα:

```
root@kali:~# nmap -sSU --top-ports 100 --open 192.168.85.*
```

Παρατηρήστε ότι με την παραπάνω εντολή ελέγχουμε τα 100 πιο δημοφιλή TCP ports (-sS) αλλά και τα 100 πιο δημοφιλή UDP ports (-sU), καθώς κι ότι συμπτύξαμε τις επιλογές -sU και -sT σε μία (-sTU).

Η συνέχεια εντός

Θέλουμε να πιστεύουμε ότι το nmap έχει κεντρίσει το ενδιαφέρον σας κι ότι έχετε ήδη αρχίσει τους πειραματισμούς, στο δικό σας εικονικό εργαστήριο. Περιττό να πούμε ότι έχουν γραφτεί βιβλία γι' αυτό το θαυμάσιο εργαλείο, θα γραφτούν κι άλλα και μολαταύτα το nmap θα συνεχίσει να έχει κρυφές όψεις και να προκαλεί το θαυμασμό. Από τη μεριά μας, πέρα από αυτή τη σύντομη εισαγωγή θα θέλαμε να πούμε λίγα περισσότερα, τα οποία αρχίζουν να απομακρύνονται λίγο από τα βασικά κι απολύτως απαραίτητα. Πηγαίνετε τώρα στο άρθρο που ξεκινά από τη σελίδα 52.

Το **deltaHacker** είναι το ένα και **μοναδικό** περιοδικό με θεματολογία το ethical **hacking**, τα **δίκτυα** και την **ασφάλεια**, τον **προγραμματισμό** και τα **ηλεκτρονικά**.

Το **deltaHacker** δεν γυρνάει εδώ κι εκεί στα περίπτερα, αλλά για τρίτη χρονιά στη σειρά **έρχεται κατευθείαν σ' εσάς**.

Αν είστε από εκείνους που δεν βλέπουν τον υπολογιστή τους ως άλλη μια οικιακή συσκευή και δεν αντιμετωπίζετε το Internet ως ένα δίκτυο που αρχίζει και τελειώνει με το Facebook και το Twitter, τότε είναι **109% βέβαιο ότι θα αγαπήσετε το deltaHacker**, καθώς κι ότι θα θέλετε την παρέα του **κάθε μήνα**.

Παραγγείλετε τώρα μία από τις συμφέρουσες συνδρομές από το

http://deltahacker.gr/pdf12order
(ηλεκτρονική έκδοση)

ή από το

http://deltahacker.gr/order
(έντυπη έκδοση, έως το τεύχος 019)

Σημείωση: Την ύλη **όλων των τευχών** που έχουν κυκλοφορήσει ως τώρα μπορείτε να τη βλέπετε στο

deltahacker.gr/category/magazine-issues

Skill: Intermediate
Tags: Kali Linux, chroot jail, Session Hijacking, ARP poisoning



by Tom Cr0w

Hacking με το Android [part 2]

Η συσκευή μας με το Android σε πολύ λίγο θα αποκτήσει το Kali Linux! Αυτό το γεγονός είναι εντυπωσιακό από μόνο του, αλλά εμάς δεν μας αρκεί. Επιπρόσθετα, θα επεκταθούμε και σε μερικές ακόμα ενδιαφέρουσες εφαρμογές που φροντίζουν και για την ασφάλεια της αγαπημένης μας συσκευής.

Στο πρώτο μέρος της μίνι σειράς μας, που αρχίζει από τη σελίδα 14 του παρόντος τεύχους, γνωρίσαμε το dSploit: μια ολοκληρωμένη συλλογή εργαλείων για penetration testing. Αυτή τη φορά θα μπούμε σε λίγο πιο βαθιά νερά κι αντί για κάποια εφαρμογή θα εγκαταστήσουμε στη συσκευή μας το Kali Linux! Η μελέτη μας όμως δεν θα σταματήσει εκεί. Θα γνωρίσουμε μερικές ακόμα εφαρμογές, που φροντίζουν για την ασφάλεια του Android και παρουσιάζουν ιδιαίτερο ενδιαφέρον.

Kali Linux για ARM

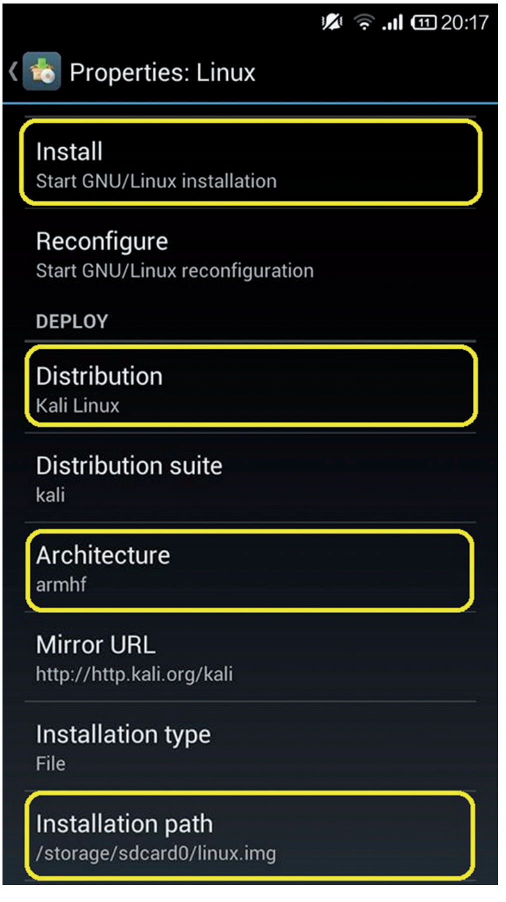
Πέραν από τις δύο κλασικές εκδοχές (x86 και x64) του Kali, από τον επίσημο δικτυακό τόπο προσφέρονται και κάποιες λιγότερο δημοφιλείς που προορίζονται για συσκευές με επεξεργαστή αρχιτεκτονικής ARM. Πρόκειται για ελαφρώς τροποποιημένες και κατάλληλα μεταγλωττισμένες εκδοχές του Kali, οι οποίες μπορούν να εκτελεστούν σε σχεδόν οποιαδήποτε συσκευή τρέχει Android! Βέβαια μη νομίσετε ότι σκοπεύουμε να ξηλώσουμε το Android από τη συσκευή μας. Εμείς, τουλάχιστον, δεν θα κάνουμε τίποτα τέτοιο. Απλά, θα τρέξουμε το Kali σ' ένα περιβάλλον chroot jail. Αν δεν έχετε υπόψη σας περί τίνος πρόκειται, να πούμε επί τροχάδην ότι το chroot jail είναι ένα απλοϊκό είδος εικονικού περιβάλλοντος, το οποίο ωστόσο δεν εκτελείται από κάποιο software hypervizor αλλά από το ίδιο το φυσικό hardware. Μήπως αυτό σας μπέρδεψε ή έστω παραξένεψε; Ένα περιβάλλον chroot jail δημιουργείται με τη διαδικασία chroot (change root), που όπως δηλώνει το όνομά της μεταβάλλει τον ριζικό κατάλογο του συστήματος αρχείων (file system root directory). Τα προγράμματα που εκτελούνται σ' ένα τέτοιο περιβάλλον αντιλαμβάνονται ως ρίζα του συστήματος αρχείων τον κατάλογο που έχουμε επιλέξει και δεν έχουν πρόσβαση στους καταλόγους και στα αρχεία που βρίσκονται "πάνω" από αυτόν τον κατάλογο. Επιπρόσθετα, σ' ένα chroot jail μπορούμε να τροποποιήσουμε κι άλλες μεταβλητές περιβάλλοντος (environment variables), όπως εκείνη που διατηρεί το home directory του λογαριασμού μας (HOME), τον προεπιλεγμένο επεξεργαστή κειμένου (EDITOR), το κέλυφος που χρησιμοποιείται για τη γραμμή εντολών (SHELL), τους καταλόγους όπου αναζητούνται τα εκτελέσιμα αρχεία (PATH) κ.ά. Αν ούτε και τώρα δεν έχετε καταλάβει τι είναι αυτά τα chroot jails, μην ανησυχείτε καθόλου. Οι θεωρητικές περιγραφές δεν αρκούν από μόνες τους. Ο καλύτερος τρόπος για να κατανοήσει κανείς τη φύση και τη χρησιμότητα των chroot jails είναι να υλοποιήσει ένα τέτοιο περιβάλλον χειροκίνητα και να το χρησιμοποιήσει[1]. Για την εργασία που εξετάζουμε θα στηριχτούμε σε εργαλεία που αυτοματοποιούν πλήρως τη δημιουργία chroot jail.

Ας επανέλθουμε τώρα στο Kali Linux. Οι εκδοχές που προορίζονται για συστήματα αρχιτεκτονικής ARM, όπως κι όλες οι υπόλοιπες άλλωστε, είναι κατασκευασμένες για να εγκαθίστανται και να ξεκινούν κανονικά. Με άλλα λόγια, δεν προορίζονται για εκτέλεση μέσα σε chroot jail. Αυτό σημαίνει ότι για να πετύχουμε το σκοπό μας χρειάζεται να τροποποιηθούν πολλά αρχεία της διανομής. Στο παρελθόν, η σχετική διαδικασία γινόταν χειροκίνητα από κάθε ενδιαφερόμενο και, όπως καταλαβαίνετε, ήταν αρκετά επίπονη. Τώρα πια το PlayStore διαθέτει αρκετές εφαρμογές που πραγματοποιούν τη μετατροπή αυτόματα. Οι περισσότερες από αυτές ετοιμάζουν ένα νέο image της διανομής, με όλες τις τροποποιήσεις και τις απαραίτητες ρυθμίσεις ώστε το σύστημα να εκτελείται κανονικά μέσα σε ένα chroot jail. Εμείς θα στηριχτούμε σε μια εφαρμογή που έχει "εγκριθεί" κι από το επίσημο blog του Kali Linux. Αναφερόμαστε στο Linux Deploy, το οποίο μπορούμε να κατεβάσουμε δωρεάν από το PlayStore. Πριν προχωρήσουμε, οφείλουμε να σημειώσουμε ότι το εγχείρημα

1. Εγκαθιστώντας, για παράδειγμα, το Gentoo Linux ή το Arch Linux χωρίς τη βοήθεια κάποιου installer, ξεκινώντας τον υπολογιστή από ένα δισκάκι CD ή από ένα USB stick με κάποια live διανομή Linux κ.ο.κ.

που περιγράφουμε δεν θα πετύχει σε οποιαδήποτε συσκευή. Για την ακρίβεια, η λειτουργία του Kali μέσα σε chroot jail θα πετύχει μόνον αν η συσκευή μας έχει τα ακόλουθα χαρακτηριστικά:

- τρέχει Android 2.1 ή νεότερο
- στηρίζεται σε επεξεργαστή ARM με τουλάχιστον δύο πυρήνες και συχνότητα λειτουργίας στα 1.2GHz
- διαθέτει τουλάχιστον 1GB RAM
- έχει τουλάχιστον 5GB ελεύθερου αποθηκευτικού χώρου.



Στο μενού εγκατάστασης του Linux Deploy έχουμε διαλέξει το Kali Linux με αρχιτεκτονική την armhf κι έχουμε καθορίσει το path όπου θέλουμε να εγκατασταθεί η διανομή (εσωτερική ή εξωτερική μνήμη). Πατώντας στο κουμπί Install ξεκινά η πολύ απλή εγκατάσταση του Kali Linux στη συσκευή μας...

Εγκατάσταση του Kali

Αφού εγκαταστήσουμε την εφαρμογή Linux Deploy στη συσκευή μας, δεν χρειάζεται να κάνουμε πολλά πράγματα. Αρχικά ανοίγουμε την εφαρμογή, μεταβαίνουμε στο μενού εγκατάστασης (βέλος με φορά προς τα κάτω) και στην καρτέλα Distribution επιλέγουμε το Kali Linux. Στη συνέχεια πρέπει να επιλέξουμε την επιθυμητή εκδοχή της διανομής. Το Kali Linux για ARM διατίθεται σε δύο εκδοχές: Μια για την αρχιτεκτονική armel και μια για την αρχιτεκτονική armhf. Η πρώτη (armel) προορίζεται για συσκευές με σχετικά παλιό hardware, οι οποίες στηρίζονται σε επεξεργαστές ARMv4. Η δεύτερη (armhf) προορίζεται για σύγχρονες συσκευές, που στηρίζονται σε επεξεργαστές ARMv7. Προφανώς, εδώ ο καθένας θα πρέπει να επιλέξει την κατάλληλη εκδοχή του Kali, ανάλογα με τα χαρακτηριστικά της συσκευής του. Ακολούθως επιλέγουμε τη θέση (path) όπου θέλουμε να αποθηκευτεί το image της διανομής. Αφού πραγματοποιήσουμε τις παραπάνω ρυθμίσεις με προσοχή, αρκεί να πατήσουμε το κουμπί Install. Το Linux Deploy θα κατεβάσει το απαραίτητο image file και θα πραγματοποιήσει αυτόματα όλες τις απαιτούμενες τροποποιήσεις! Σημειώστε ότι η εφαρμογή θα κατεβάσει περίπου 1,4GB δεδομένων. Επομένως, γι' αυτό το τελικό βήμα, θα είναι φρόνιμο —αν όχι απαραίτητο— να έχουμε συνδεθεί στο Internet μέσω κάποιου δικτύου WiFi.

Μετά από λίγη ώρα κι εφόσον έχουν πάει όλα καλά, θα εμφανιστεί το ακόλουθο μήνυμα:

```
<<< end:
```

Εφόσον η λήψη και η τροποποίηση του αρχικού image file ολοκληρώθηκαν με επιτυχία, μπορούμε να προχωρήσουμε στην εκκίνηση του Kali. Φυσικά, γι' αυτό το σκοπό θα στραφούμε και πάλι στο Linux Deploy, όπου αρκεί να πατήσουμε το κουμπί Start στο κεντρικό μενού. Το πρόγραμμα θα πραγματοποιήσει ένα mount του τροποποιημένου image, θα δημιουργήσει το κατάλληλο chroot jail και στο πλαίσιό του θα ξεκινήσει τις υπηρεσίες SSH και VNC. Αυτό ήταν όλο! Πλέον, μπορούμε να συνδεθούμε στο Kali Linux από οποιονδήποτε υπολογιστή βρίσκεται στο ίδιο τοπικό δίκτυο με την συσκευή μας, όπως επίσης κι από την ίδια τη συσκευή.

Προφανώς, εφόσον ο στόχος μας είναι η χρήση του Kali από τη συσκευή, πρέπει να εγκαταστήσουμε μια εφαρμογή VNC. Εμείς προτείνουμε την bVNC Free, από το PlayStore. Εκτός του ότι είναι δωρεάν, επιτρέπει τη λειτουργία σε full-screen mode και υποστηρίζει το χειρισμό του "απομακρυσμένου" συστήματος με τη χρήση touchpad ή mouse. Εξάλλου, η ίδια η εφαρμογή ενσωματώνει virtual keyboard και virtual mouse pad. Οι ρυθμίσεις που πρέπει να πραγματοποιήσουμε στην εφαρμογή VNC (όποια κι αν τελικά επιλέξουμε) είναι οι εξής:

- IP/Host: localhost ή 127.0.0.1
- Port: 5900
- Password: changeme

Αφού συνδεθούμε στο Kali Linux μέσω VNC, το πρώτο πράγμα που πρέπει να κάνουμε είναι να ενημερώσουμε το σύστημα και να προσθέσουμε τα απαραίτητα εργαλεία. Βλέπετε, η συγκεκριμένη εκδοχή του Kali Linux δεν περιλαμβάνει κανένα από τα εργαλεία που το καθιστούν ιδανικό για penetration testing. Γι' αυτό το λόγο πρέπει να εκτελέσουμε τα ακόλουθα:

```
sudo apt-get update
sudo apt-get upgrade
sudo apt-get install kali-linux –yq
```

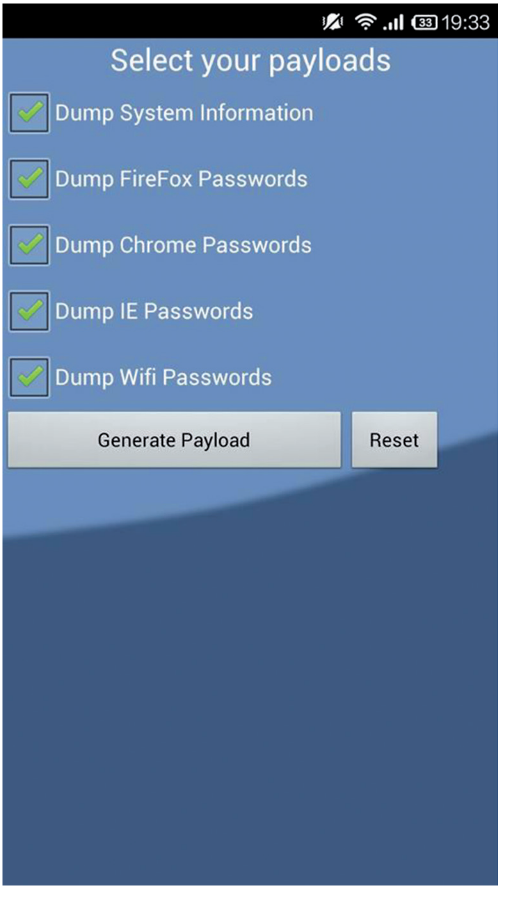
Αν κατά τη διάρκεια των παραπάνω εγκαταστάσεων παρουσιαστεί κάποιο σφάλμα σχετικό με την PostgreSQL, θα χρειαστεί να δώσουμε το εξής:

```
sudo usermod -a -G aid_inet postgres
```

Όταν ολοκληρωθούν οι παραπάνω διαδικασίες, η συσκευή μας θα διαθέτει μια πλήρως λειτουργική εγκατάσταση του Kali Linux! Σημειώστε ότι αν θέλετε να συνδεθείτε μέσω SSH, θα πρέπει να χρησιμοποιήσετε σαν username το "android" κι ως password το "changeme" (τουλάχιστον μέχρι να το αλλάξετε ;))

Στην πράξη

Παίζοντας με την εγκατάσταση του Kali, εντοπίσαμε ορισμένα μικροπροβλήματα που οφείλονταν κυρίως στην περιορισμένη ισχύ της συσκευής. Μεταξύ άλλων, όμως, συναντήσαμε προβλήματα και με την εκκίνηση του browser, τα οποία δεν σχετίζονταν με την ισχύ της συσκευής αλλά με την ίδια την εγκατάσταση του browser (IceWeasel). Αν τα συναντήσετε κι εσείς, αρκεί να προβείτε σε μια πλήρη απεγκατάσταση και κατόπιν σε μια εκ νέου εγκατάσταση:



Η λίστα με τα payloads που μπορεί να δημιουργήσει η πιο πρόσφατη έκδοση του USB Cleaver.

```
sudo apt-get purge iceweasel
sudo apt-get install iceweasel
```

Ας περάσουμε όμως σε κάτι πολύ πιο ενδιαφέρον. Κάτι που μας χαροποίησε ιδιαίτερα, ήταν η άριστη λειτουργία της πλατφόρμας Aircrack-NG σε συνεργασία με μια εξωτερική κάρτα ασύρματης δικτύωσης. Για τις δοκιμές μας χρησιμοποιήσαμε την κάρτα Alfa AWUS036H, η οποία υποστηρίζει τη λειτουργία monitor mode και διευκολύνει την παρακολούθηση όλων των διακινούμενων πακέτων. Για τη σύνδεση της κάρτας χρησιμοποιήσαμε ένα καλώδιο OTG (αρσενικό micro-USB και θηλυκό USB), ενώ χρησιμοποιήσαμε και μια εξωτερική πηγή τροφοδοσίας, ώστε ν' αποφύγουμε τυχόν προβλήματα με τη συσκευή.

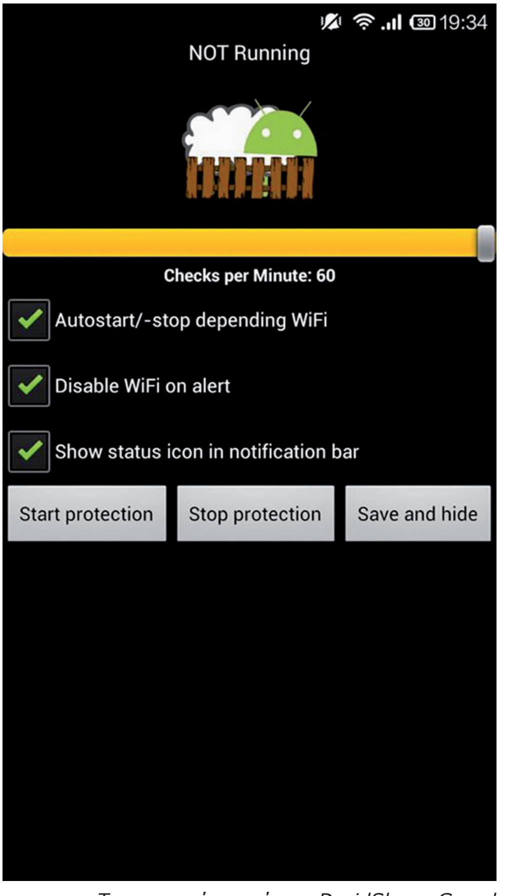
Αφού συνδέσαμε την εξωτερική κάρτα ασύρματης δικτύωσης, εκκινήσαμε το Kali και στη συνέχεια ενεργοποιήσαμε το παραθυρικό του περιβάλλον, δίνοντας ένα startx. Ακολούθως ανοίξαμε ένα παράθυρο τερματικού και πληκτρολογήσαμε ένα ifconfig. Έτσι, εντοπίσαμε την ύπαρξη ενός νέου network interface, που στην περίπτωση μας ήταν το wlan0. Για να θέσουμε την κάρτα σε monitor mode καταφύγαμε στο πρόγραμμα airmon:

```
airmon-ng wlan0 start
```

Μετά το παραπάνω κι εκτελώντας εκ νέου το ifconfig, παρατηρήσαμε ότι είχε προκύψει κι ένα πρόσθετο network interface, με το όνομα mon0. Με τη βοήθεια αυτού του interface μπορούσαμε να εκτελέσουμε πλέον κάθε επίθεση που ενσωματώνει η πλατφόρμα Aircrack-NG! Έτσι, παρά τους ισχυρισμούς κάποιων ότι οι επιθέσεις σε ασύρματα δίκτυα είναι αδύνατες με συσκευές που τρέχουν Android, εμείς τα καταφέραμε. Φυσικά, πρέπει να σημειώσουμε ότι η αποτελεσματικότητα πολλών επιθέσεων καθορίζεται σε μεγάλο βαθμό από την ισχύ της συσκευής. Επίσης, σκεφτείτε ότι πίσω από το Kali Linux τρέχει το Deploy Linux (για την εκκίνηση του Kali), καθώς και το bVNC Free. Μια καλή ιδέα για να ελαφρύνουμε το λειτουργικό σύστημα της συσκευής μας θα ήταν η χρήση του SSH.

Ύπουλη κλοπή

Όσοι γνωρίζουν τις εφαρμογές USB Haksaw και USB Switchblade, ξέρουν ήδη σε τι αναφερόμαστε. Για όσους δεν γνωρίζουν, να πούμε ότι το USB Cleaver αποτελεί μια εφαρμογή για το Android η οποία δημιουργεί payloads για την κλοπή κωδικών κι άλλων πληροφοριών από υπολογιστές που τρέχουν Windows 2000 ή κάτι νεότερο. Τα δεδομένα που μπορούν να αποκτηθούν με αυτόν τον τρόπο είναι τα χαρακτηριστικά του συστήματος, οι αποθηκευμένοι κωδικοί σε Internet Explorer, Chrome ή Firefox, καθώς και οι κωδικοί για τη σύνδεση σε ασύρματα δίκτυα. Μάλιστα, σε μελλοντικές εκδόσεις του προγράμματος αναμένεται να προστεθούν payloads για την υποκλοπή μιας ευρύτερης γκάμας δεδομένων.



Το κεντρικό μενού του DroidSheep Guard περιλαμβάνει μερικές χρήσιμες ρυθμίσεις, καθώς κι ένα κυλιόμενο ρυθμιστικό για να καθορίζουμε το πόσο συχνά θα εκτελούνται οι έλεγχοί του.

Η λειτουργία του USB Cleaver είναι εξαιρετικά απλή. Αφού ανοίξουμε την εφαρμογή επιλέγουμε τα δεδομένα που θέλουμε να κλέψουμε, πατάμε το κουμπί Generate Payload και στη συνέχεια το Enable/disable payloads. Κατ' αυτόν τον τρόπο δημιουργείται το κατάλληλο payload και τοποθετείται στο ριζικό κατάλογο της κάρτας μνήμης της συσκευής. Πρόκειται για ένα αρχείο BAT (go.bat), που αν το εκτελέσουμε σε κάποιο σύστημα με Windows θα συλλέξει τα επιθυμητά δεδομένα και θα τα αποθηκεύσει σε ένα αρχείο απλού κειμένου. Αν θέλουμε να κάνουμε τα πράγματα λίγο πιο ενδιαφέροντα, μπορούμε να εκμεταλλευτούμε και τη λειτουργία αυτόματης εκκίνησης των Windows. Για το σκοπό αυτό αρκεί να δημιουργήσουμε ένα αρχείο με το όνομα "autorun.inf" και να το τοποθετήσουμε στον ίδιο κατάλογο με το go.bat (στον ριζικό κατάλογο της κάρτας μνήμης). Μέσα στο εν λόγω αρχείο πρέπει να προσθέσουμε τα ακόλουθα:

```
[autorun]
open=go.bat
```

Εφόσον έχουμε φτιάξει το autorun.inf, κάθε φορά που συνδέουμε τη συσκευή μας σε υπολογιστή με Windows, το σύστημα θα μας ρωτά για το αν θέλουμε να εκτελεστεί το go.bat. Εξαίρεση αποτελούν τα Windows XP, όπου η εκτέλεση του go.bat θα ξεκινά αυτόματα και, χωρίς καμία απολύτως προειδοποίηση. Όπως αντιλαμβάνεστε, αν ο ιδιοκτήτης του υπολογιστή είναι λίγο αφηρημένος, ο κάτοχος ενός smartphone

που χρησιμοποιεί το USB Cleaver θα μπορούσε να κλέψει κρίσιμα δεδομένα, με μεγάλη άνεση.

Η εφαρμογή βρίσκεται σε φάση Beta — και δεν ξέρουμε αν θα βγει ποτέ απ' αυτή :P Μπορείτε να κατεβάσετε το αρχείο APK με την πιο πρόσφατη έκδοση από τη διεύθυνση `https://bit.ly/1tYfFgM`.

Περιοδικοί, προληπτικοί έλεγχοι

Το DroidSheep και το DroidSheep Guard αποτελούν τα προϊόντα της πτυχιακής εργασίας του Andrea Koch. Πρόκειται για δύο εφαρμογές που δημιουργήθηκαν με σκοπό να αποδείξουν πόσο εύκολη είναι η πραγματοποίηση αλλά και η απόκρουση ενός συγκεκριμένου είδους επιθέσεων. Παρ' όλα αυτά, παρουσιάζουν αυξημένο ενδιαφέρον και χρησιμότητα.

Το DroidSheep αποτελεί ένα μικρό κι ελαφρύ πρόγραμμα που πραγματοποιεί επιθέσεις Session Hijacking. Ο στόχος του είναι να αναδείξει πόσο εύκολα πραγματοποιούνται αυτές οι επιθέσεις και, ταυτόχρονα, πόσο επικίνδυνες είναι. Το Session Hijacking προβλέπει την κλοπή των cookies που αντιστοιχούν σε ενεργά sessions του browser του θύματος. Με τη βοήθεια αυτών των cookies ο επιτιθέμενος μπορεί να συνδεθεί στις υπηρεσίες που έχει συνδεθεί και το θύμα, με το λογαριασμό του τελευταίου και χωρίς να δώσει κάποιον κωδικό! Φυσικά αυτή η επίθεση επιτυγχάνει υπό προϋποθέσεις, αλλά ο κίνδυνος δεν παύει να είναι υπαρκτός.

Για τη λειτουργία του DroidSheep η συσκευή μας πρέπει να είναι rooted. Η χρήση του όμως είναι εξαιρετικά απλή. Αρκεί ν' αναφέρουμε ότι το περιβάλλον του προγράμματος περιλαμβάνει μόνο ένα κουμπί για την εκκίνηση της επίθεσης και δύο επιλογές. Η μία από αυτές καθορίζει το αν ταυτόχρονα με το Session Hijacking θα πραγματοποιείται και ένα ARP poisoning. Η άλλη καθορίζει το αν θα εμφανίζονται και θα υποκλέπτονται τα cookies από *όλα* τα sessions ή μόνο από εκείνα των δημοφιλών δικτυακών υπηρεσιών. Μπορούμε να κατεβάσουμε το πακέτο εγκατάστασης του DroidSheep από το επίσημο thread στο XDA-Developers: `https://bit.ly/1q3pQAv`.

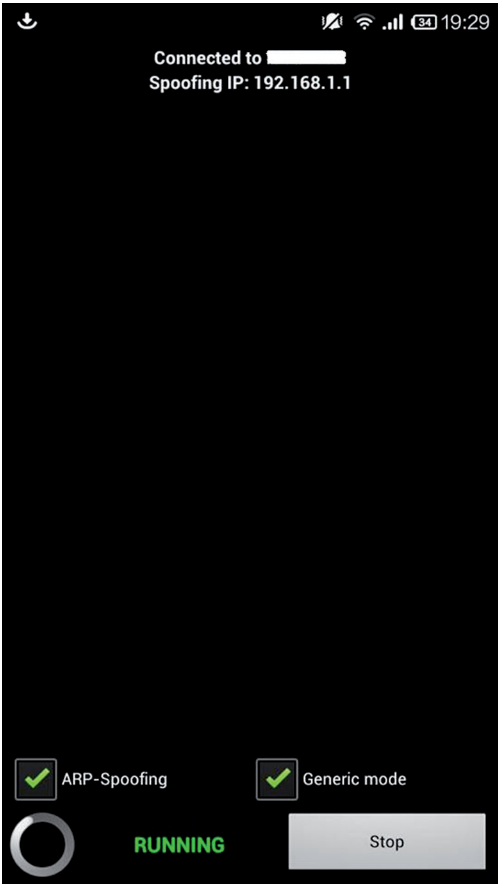
Το δε DroidSheep Guard αποτελεί την απάντηση στις επιθέσεις Session Hijacking. Το εν λόγω πρόγραμμα εκτελείται στο παρασκήνιο του συστήματος κι ελέγχει, σε τακτά χρονικά διαστήματα, τα περιεχόμενα του ARP table της συσκευής μας. Όσο τα πράγματα δείχνουν φυσιολογικά η εφαρμογή δεν κάνει τίποτα. Αντίθετα, στην περίπτωση που παρατηρηθούν ύποπτες αλλαγές στο ARP table, η εφαρμογή ειδοποιεί το χρήστη για τον ενδεχόμενο κίνδυνο να αποτελεί θύμα μιας επίθεσης ARP poisoning. Στη συνέχεια εκτελούνται και οι ενέργειες που έχει επιλέξει ο χρήστης από τις ρυθμίσεις του προγράμματος. Η χρήση του DroidSheep Guard είναι επίσης πανεύκολη. Από τις ρυθμίσεις του μπορούμε να καθορίσουμε το αν θα ξεκινά αυτόματα κάθε φορά που ενεργοποιούμε το WiFi, το αν θα πραγματοποιείται αποσύνδεση από το δίκτυο όταν δεχόμαστε επίθεση και το αν θα εμφανίζεται ένα σχετικό εικονίδιο στην περιοχή ειδοποιήσεων του συστήματος. Επιπρόσθετα, από τις ρυθμίσεις του προγράμματος μπορούμε να επιλέξουμε και το πόσο συχνά θα πραγματοποιούνται οι έλεγχοί του (πόσες φορές το λεπτό). Εν ολίγοις, θα μπορούσαμε να πούμε ότι πρόκειται για μια χρήσιμη εφαρμογή που καλό θα ήταν να εγκαθιστούμε σε κάθε συσκευή με Android. Εξάλλου, σε αντίθεση με το DroidSheep, το DroidSheep Guard διανέμεται κι εγκαθίσταται πανεύκολα από το PlayStore.

...κι ένα φιλικό μήνυμα ;)

Τα εργαλεία που παρουσιάσαμε είναι εκείνα που εμείς θεωρούμε αξιόλογα, αλλά δεν είναι τα μοναδικά. Όπως και να 'χει, είτε χρησιμοποιήσετε τις συγκεκριμένες εφαρμογές είτε προτιμήσετε κάποιες άλλες, θα πρέπει να είσαστε ιδιαίτερα προσεκτικοί. Η χρήση τέτοιων εργαλείων θα πρέπει να γίνεται μόνο κατόπιν εξουσιοδοτήσεως από τον ιδιοκτήτη του εκάστοτε δικτύου και των συσκευών-στόχων. Από αυτόν τον κανόνα εξαιρείται μόνο το

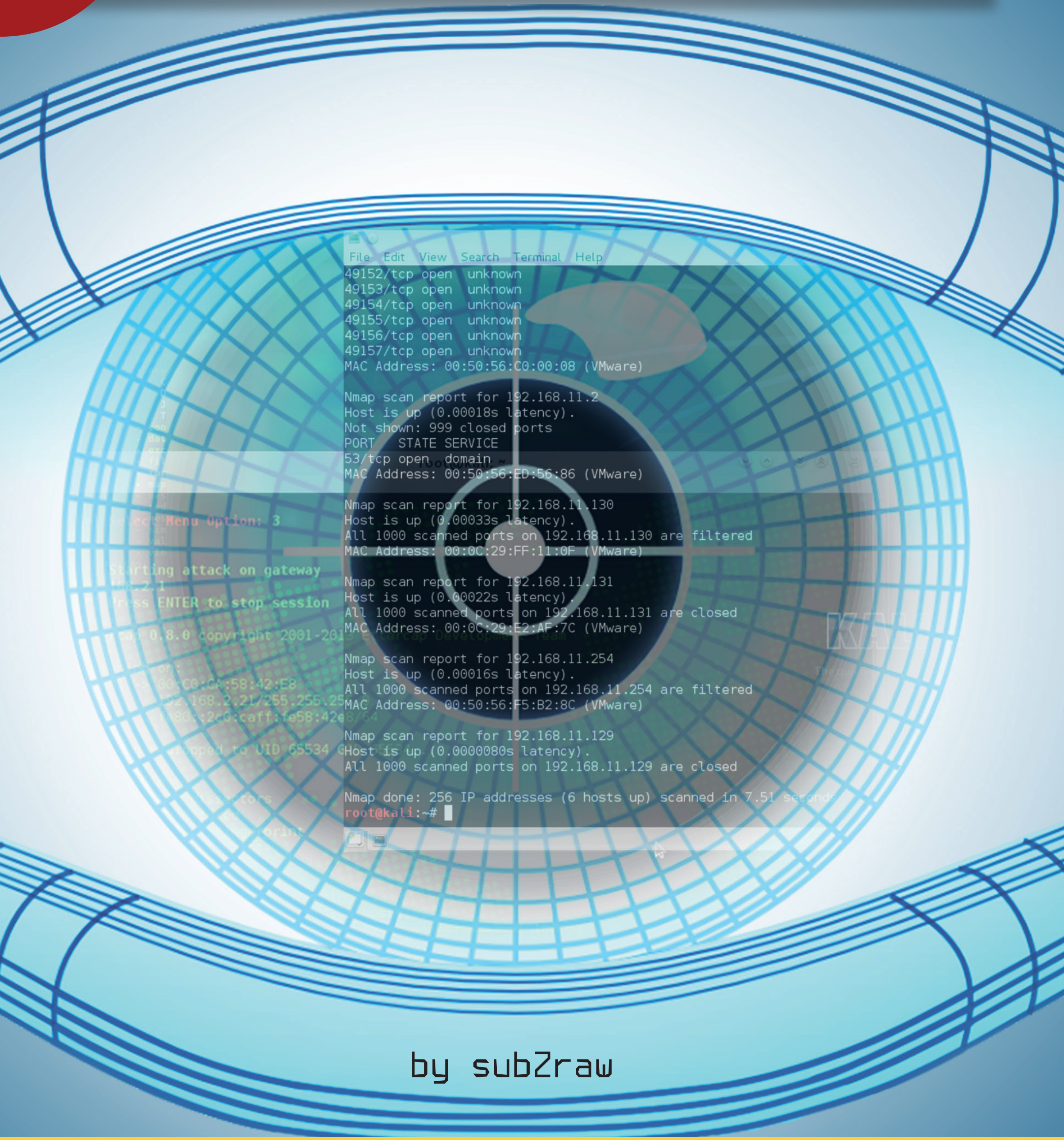
DroidSheep Guard, αφού δεν "κρυφακούει", δεν "εξαπατά" και δεν επιτίθεται σε κανέναν.

Πέρα από οποιαδήποτε τεχνική γνώση ή ιδέα μπορεί ν' αποκτήσατε διαβάζοντας τα δύο άρθρα της μίνι σειράς μας, ελπίζουμε να βγάλατε κι ένα βασικό συμπέρασμα: Ζούμε στην εποχή κατά την οποία ο στιλάτος νέος που κάθεται στο απέναντι τραπέζι τις καφετέριας δεν είναι σίγουρο ότι κάνει check-in στο Facebook. Ενδέχεται να έχει εξαπολύσει μια πληθώρα επιθέσεων στο δίκτυο της καφετέριας, πίνοντας χαλαρά το καφεδάκι του και κοιτώντας αμέριμνα τη θάλασσα. Έτσι τουλάχιστον κάνουν κάποιοι εδώ, στον βορρά ;)



Το λιτό αλλά λειτουργικό user interface του DroidSheep. Με ένα μόνο κουμπί και δυο checkboxes μπορεί κι εξαπολύει πανίσχυρες επιθέσεις Session Hijacking!

Skill: Intermediate
Tags: nmap, 3-way handshake, timing, scripting engine, NSE scripts



by subZraw

Το nmap πέρα από τα βασικά

Μετά την πρώτη γνωριμία με το θαυμαστό nmap παραμένουμε στο άνετο περιβάλλον του Kali Linux και συνεχίζουμε τους πειραματισμούς στο πλαίσιο του εικονικού μας εργαστηρίου. Έχει φτάσει η ώρα να δούμε κάποιες πιο προχωρημένες δυνατότητες του nmap και να εκμεταλλευτούμε την πανίσχυρη scripting engine του προγράμματος. Τι λέτε, παίζουμε;

Σε όσα video tutorials (http://deltahacker.gr/category/deltacast) ασχολούμαστε με το pen-testing, σίγουρα θα έχετε παρατηρήσει ότι σκανάρουμε το τοπικό δίκτυο για υποψήφιους στόχους πληκτρολογώντας κάτι τέτοιο:

```
root@kali:~# nmap -sS -Pn -T4 -A 10.10.10.0/24
```

Σε σχέση με όσα έχουμε δει στο εισαγωγικό άρθρο που ξεκινά από τη σελίδα 24, στην παραπάνω εντολή υπάρχουν δύο νέες επιλογές: -A και -T4. Επίσης, αν και κάθε φορά που τρέχουμε το nmap ως root η επιλογή -sS υπονοείται, παραπάνω τη συμπεριλάβαμε σκόπιμα διότι θέλουμε να συζητήσουμε για ορισμένες μεθόδους port scanning. Ας αρχίσουμε λοιπόν απ' αυτό το τελευταίο: την επιλογή -sS και τη σημασία της.

Κάθε φορά που πρόκειται να εγκαθιδρυθεί μια σύνδεση TCP μεταξύ δύο hosts A και B, λαμβάνει χώρα μια προκαταρκτική διαδικασία που ονομάζεται 3-way handshake. Ας υποθέσουμε ότι, για κάποιο λόγο, ο host A θέλει να συνδεθεί στον host B. Μπορούμε, π.χ., να φανταζόμαστε τον A ως τον client και τον B ως τον server. Παρακολουθήστε τη διαδικασία του 3-way handshake:

1. Ο A στέλνει σε κάποιο port του B ένα πακέτο TCP SYN (το SYN προέρχεται από το SYNchronize). Ο B λαμβάνει το πακέτο.
2. Ο B στέλνει στον A ένα πακέτο SYN/ACK (το ACK προέρχεται από το ACKnowledge). Ο A λαμβάνει το πακέτο SYN/ACK.
3. Ο A στέλνει στον B ένα πακέτο ACK. Ο B λαμβάνει το πακέτο ACK.

Μετά και το βήμα 3 εγκαθιδρύεται μια σύνδεση μεταξύ των A και B. Κοιτάξτε τώρα τι συμβαίνει όποτε δίνουμε στο nmap την επιλογή -sS: Για κάθε port που ελέγχουμε, το nmap ξεκινά ένα 3-way handshake αλλά δεν το ολοκληρώνει ποτέ. Αντίθετα, φτάνει μέχρι το βήμα 2 κι εξετάζει την απάντηση του στόχου. Αναλυτικότερα:

- αν λάβει ένα πακέτο SYN/ACK, τότε το υπό εξέταση port είναι ανοικτό
- το port θεωρείται ως ανοικτό και στη σπάνια περίπτωση μιας σύνδεσης split handshake, κατά την οποία ο client αντί για SYN/ACK λαμβάνει ένα πακέτο SYN (βλ. και http://nmap.org/misc/split-handshake.pdf)
- αν το nmap λάβει ένα πακέτο RST (από το reset) τότε το port είναι μάλλον κλειστό, δηλαδή δεν υπάρχει κάποια υπηρεσία που να το χρησιμοποιεί
- αν μετά από αρκετές προσπάθειες το nmap δεν λάβει κάποια απάντηση, τότε το port χαρακτηρίζεται ως filtered
- ως filtered χαρακτηρίζεται κι όποτε συμβαίνει ένα λάθος τύπου ICMP unreachable.

Ακριβώς επειδή η συγκεκριμένη τεχνική σάρωσης του nmap σταματάει πάντα στο βήμα 2 του 3-way handshake, ονομάζεται half-open scanning. Αποτελεί δε την πλέον δημοφιλή τεχνική, αφού είναι σχετικά γρήγορη κι αυτό που θα λέγαμε "stealthy", ενώ το μόνο που απαιτείται για να δουλέψει είναι μια τυπική στοίβα TCP/IP — το λειτουργικό που τρέχει ο στόχος δεν έχει σημασία!

Όταν δεν είναι δυνατή η ενεργοποίηση του half-open scanning, π.χ., επειδή το nmap δεν τρέχει από το λογαριασμό του υπερχρήστη, τότε εξ ορισμού χρησιμοποιείται το λεγόμενο TCP connect scan (επιλογή -sT). Με αυτή την τεχνική το nmap εγκαθιδρύει κανονικές, πλήρεις συνδέσεις προς τα ports του στόχου, και με βάση τα πακέτα που

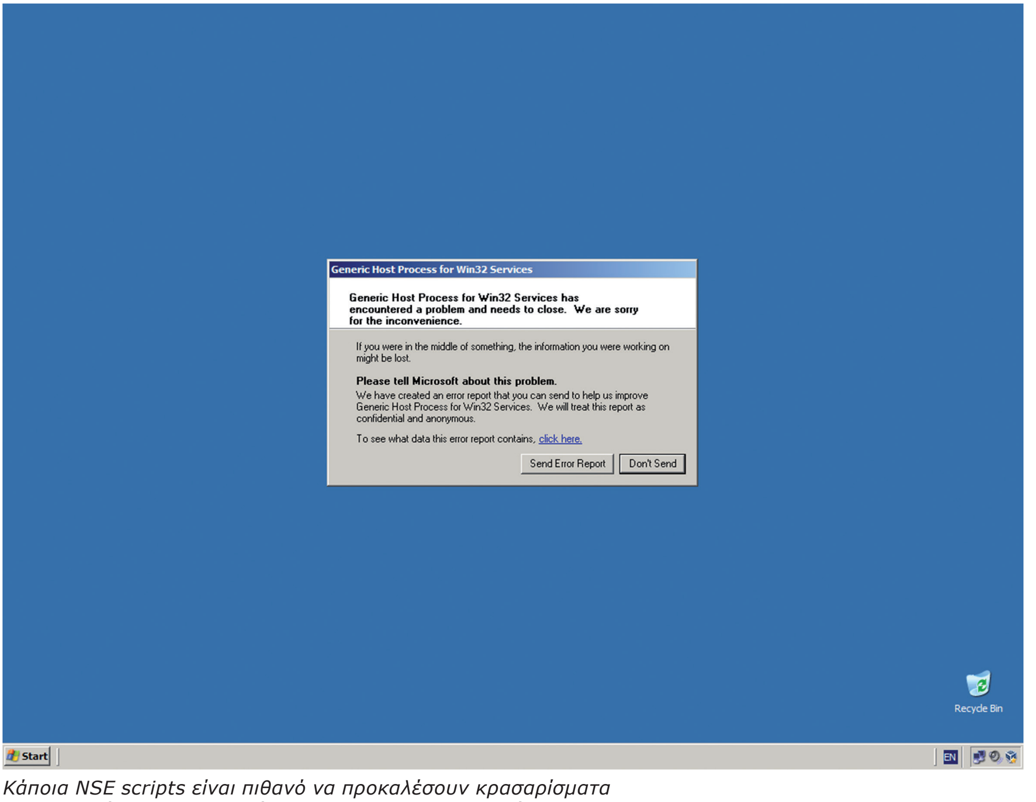
λαμβάνει επιχειρεί να συναγάγει τις όποιες πληροφορίες του έχουμε ζητήσει (π.χ., εκδόσεις ενεργών υπηρεσιών). Ένα TCP connect scan είναι πιο αργό σε σύγκριση με ένα TCP SYN scan προς το ίδιο μηχάνημα. Επίσης, ακόμη κι αν ο στόχος δεν τρέχει κάποιο IDS, η ίδια η πράξη του σαρώματος είναι πολύ πιθανό να αποθηκευτεί στα σχετικά αρχεία καταγραφής (log files).

Υπάρχουν κι άλλες τεχνικές σάρωσης που υποστηρίζει το nmap, όπως, π.χ., οι TCP Window scan (-sW) και TCP Maimon scan (-sM), οι οποίες αμφότερες εκμεταλλεύονται λεπτομέρειες υλοποίησης της στοίβας TCP/IP στα λειτουργικά των στόχων. Να σημειώσουμε τέλος ότι το nmap επιτρέπει στο χρήστη να καθορίζει ο ίδιος τις τιμές των flags στα TCP packets που αποστέλλονται στους στόχους (επιλογή --scanflags). Σίγουρα πρόκειται για προχωρημένη δυνατότητα που ενδιαφέρει όσους έχουν εμβαθύνει στο πρωτόκολλο TCP και ξέρουν πολύ καλά τι κάνουν.

Ανεξαρτήτως του τύπου σάρωσης και του πόσο εξειδικευμένα scans θέλετε να δοκιμάσετε, το man page του nmap είναι αρκετά καλογραμμένο και μάλλον περιλαμβάνει περισσότερες πληροφορίες απ' όσες θα περιμένατε ;) Πληκτρολογήστε

```
root@kali:~# man nmap
```

για περισσότερα.



Κάποια NSE scripts είναι πιθανό να προκαλέσουν κρασαρίσματα στα μηχανήματα που σκανάρουμε. Στο screenshot βλέπουμε τα αποτελέσματα του smb-check-vulns σε ένα host με Windows XP.

Ζητήματα χρόνου

Ο παράγοντας της ταχύτητας είναι μεγίστης σημασίας για το nmap. Όπως πιθανώς έχετε διαπιστώσει σκανάροντας κάποια hosts στο τοπικό σας δίκτυο, όταν, π.χ., ελέγχετε ένα μόνο μηχάνημα τότε η σάρωση συχνά ολοκληρώνεται σε κλάσματα του δευτερολέπτου. Τα πράγματα όμως αλλάζουν δραμματικά όποτε χρειάζεται να σαρώνουμε εκατοντάδες ή χιλιάδες hosts. Επίσης, ένα UDP scan είναι από τη φύση του πολύ πιο αργό σε σύγκριση με ένα TCP scan. Σημαντικά επηρεάζει την ταχύτητα σάρωσης και το τι ζητάμε από το nmap. Τις φορές, π.χ., που ενεργοποιούμε το μηχανισμό εντοπισμού της έκδοσης των υπηρεσιών, ο χρόνος ολοκλήρωσης αυξάνει σημαντικά.

Αν και το nmap υλοποιεί έξυπνα τρικ και τεχνικές προκειμένου να επιταχύνει τις σαρώσεις, την ίδια στιγμή προσφέρει στο χρήστη και τη δυνατότητα παρέμβασης στον τρόπο κατά τον οποίο το πρόγραμμα λειτουργεί. Υπάρχει μια πληθώρα επιλογών γι' αυτό το σκοπό (--min-hostgroup, --max-hostgroup, --min-parallelism, --max-parallelism, --max-retries, --host-timeout κ.ά.) κι ο ενδιαφερόμενος χρήστης καλείται να πειραματιστεί με την ησυχία του, ώστε να δει τι αποτελέσματα μπορεί να έχει σε διαφορετικά περιβάλλοντα. Όμως με όλες αυτές τις —δεκατέσσερις στο πλήθος— διαφορετικές επιλογές, υπάρχουν και δύο θέματα:

- είναι πολλές και συχνά μπερδεύουν
- δύσκολα αξιολογούνται οι επιδράσεις τους στην πράξη, ειδικά όταν ο pentester ούτως ή άλλως έχει περιορισμένο χρόνο για να κάνει την εργασία του.

Ευτυχώς, το nmap παρέχει έξι διαφορετικά πρότυπα χρονισμού (timing templates). Ουσιαστικά πρόκειται για έξι διαφορετικά σύνολα προεπιλογών, τα οποία τίθενται σε ισχύ με τη βοήθεια της επιλογής -Tx, όπου το x είναι μεταξύ των 0 και 5 συμπεριλαμβανομένων. Εναλλακτικά, ο χρήστης μπορεί να δίνει κάτι σαν -T χαρακτηρισμός, όπου ο χαρακτηρισμός είναι ένας από τους paranoid, sneaky, polite, normal, aggressive και insane. Ας δούμε για τι σενάριο/περιβάλλον προορίζεται καθένα από τα διαθέσιμα timing templates.

- **paranoid (0)** και **sneaky** (1). Πρότυπα κατάλληλα για την αποφυγή συστημάτων intrusion detection. Δεν επιτρέπουν στο nmap να διεξάγει παράλληλους ελέγχους και τα ports των στόχων δοκιμάζονται ένα προς ένα. Με το πρότυπο paranoid παρεμβάλλονται 5 λεπτά μεταξύ δύο διαδοχικών ελέγχων, ενώ με το sneaky 15 δευτερόλεπτα.
- **polite** (2). Αργό scanning ώστε να χρησιμοποιείται λιγότερο bandwidth, λιγότεροι πόροι των υπό εξέταση μηχανημάτων, καθώς και να ελαχιστοποιείται —πρακτικά να μηδενίζεται— η πιθανότητα για κάποιο crash. Με το πρότυπο polite οι έλεγχοι γίνονται επίσης εν σειρά (όχι παράλληλα) και μεταξύ τους παρεμβάλλονται 400 χιλιοστά του δευτερολέπτου.
- **normal** (3). Πρόκειται για τις προκαθορισμένες επιλογές timing που λαμβάνονται υπόψη σε κάθε σάρωση, εκτός κι αν επιλεγεί άλλο πρότυπο χρονισμού. Ένα normal scan επιτρέπει τον παραλληλισμό των ελέγχων και είναι πολύ πιθανό να ολοκληρώνεται ως και δέκα φορές γρηγορότερα, σε σύγκριση με ένα polite scan (διατηρώντας, βεβαίως, όλες τις άλλες παραμέτρους σταθερές κι επιχειρώντας εντός του ίδιου δικτύου).

- **aggressive** (4). Επιτάχυνση της διαδικασίας σάρωσης, προϋποθέτοντας ότι δουλεύουμε σ' ένα γρήγορο κι αξιόπιστο δίκτυο. Το εν λόγω timing template προτείνεται για σύγχρονα LANs αλλά και για όσους διαθέτουν μια σχετικά γρήγορη σύνδεση στο Internet, όπως, π.χ., μια αξιοπρεπή γραμμή ADSL.
- **insane** (5). Θεωρώντας ότι βρισκόμαστε σ' ένα εξαιρετικά γρήγορο δίκτυο, η επιλογή του συγκεκριμένου προτύπου συντελεί σ' ένα ταχύτατο scanning κατά το οποίο, όμως, ενδέχεται να αντληθούν λιγότερες πληροφορίες σε σύγκριση μ' αυτές που θα αντλούνταν αν είχε επιλεγεί κάποιο λιγότερο "αισιόδοξο" πρότυπο.

Έχετε υπόψη ότι τα πρότυπα χρονισμού επιτρέπεται να συνδυάζονται με επιλογές που επηρεάζουν λεπτομερώς τον τρόπο λειτουργίας του nmap (fine-grained control options). Σ' αυτές τις περιπτώσεις, οι επιλογές που κάνουμε εμείς προηγούνται σε σχέση με εκείνες που πιθανώς υπαγορεύονται από το εκάστοτε timing template. Περισσότερα θα διαβάσετε στο man page του nmap.

Επιλογή — υπερόπλο

Πάμε τώρα στην επιλογή -A, την οποία τόσες φορές έχουμε χρησιμοποιήσει στα video tutorials του περιοδικού. Ουσιαστικά, αυτό το -A δεν είναι τίποτε άλλο από μια συντόμευση για την ενεργοποίηση τεσσάρων λειτουργιών:

-O - αναγνώριση λειτουργικού συστήματος

-sV - αναγνώριση εκδόσεων υπηρεσιών

-sC - script scanning, θα πούμε περισσότερα σε λίγο

--traceroute - "χαρτογράφηση" διαδρομών από το μηχάνημα με το nmap έως τους στόχους

Λόγω της ενεργοποίησης του προκαθορισμένου συνόλου scripts (-sC), η επιλογή -A καλό είναι να μη χρησιμοποιείται σε συστήματα που δεν είναι δικά μας, τουλάχιστον όχι πριν πάρουμε άδεια για να προχωρήσουμε. Πάντως για το scanme.nmap.org όλοι έχουν άδεια σάρωσης, οπότε δείτε τι επιστρέφει η επιλογή -A:

```
root@kali:~# nmap -A -T4 scanme.nmap.org
Starting Nmap 6.47 ( http://nmap.org ) at 2014-08-30 09:32 EEST
Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.21s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 5.3p1 Debian 3ubuntu7.1 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
|_  2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
80/tcp   open  http       Apache httpd 2.2.14 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
```

```
9929/tcp open  nping-echo Nping echo
Device type: general purpose|phone|firewall
Running (JUST GUESSING): Linux 2.6.X|3.X (95%), Fortinet Linux 2.6.X
(87%), IPFire Linux 2.6.X (86%)
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3 cpe:/
o:fortinet:linux_kernel:2.6 cpe:/o:ipfire:linux:2.6.32
Aggressive OS guesses: Linux 2.6.32 - 2.6.39 (95%), 2.6.32 (94%), Linux
2.6.38 (93%), Linux 2.6.32 - 2.6.35 (92%), Linux 2.6.30 (91%), Linux
2.6.37 (91%), Linux 2.6.39 (91%), Linux 2.6.32 - 3.0 (91%), Linux 3.2 -
3.8 (90%), Linux 3.8 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 17 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 139/tcp)
HOP RTT       ADDRESS
1   14.48 ms  37.x.x.x
2   21.78 ms  78.x.x.x
3   14.88 ms  gi0-3.vxr2.skg.synapsecom.gr (78.108.32.70)
4   22.48 ms  gi0-0-0-2.rcr11.skg01.atlas.cogentco.com (149.11.72.21)
5   26.36 ms  be2297.ccr21.sof02.atlas.cogentco.com (130.117.2.41)
6   48.71 ms  be2046.ccr21.vie01.atlas.cogentco.com (130.117.1.22)
7   44.15 ms  be2200.ccr21.muc01.atlas.cogentco.com (130.117.49.1)
8   56.58 ms  be2229.ccr42.fra03.atlas.cogentco.com (154.54.38.57)
9   57.82 ms  be2188.agr21.fra03.atlas.cogentco.com (130.117.48.113)
10  48.13 ms  telia.fra03.atlas.cogentco.com (130.117.14.90)
11  50.46 ms  ffm-bb2-link.telia.net (213.155.136.198)
12  134.79 ms nyk-bb1-link.telia.net (213.155.131.145)
13  221.58 ms sjo-bb1-link.telia.net (80.91.245.96)
14  217.72 ms hurricane-ic-138359-sjo-bb1.c.telia.net (213.248.67.106)
15  211.98 ms 10ge3-2.core3.fmt2.he.net (184.105.222.13)
16  212.23 ms router3-fmt.linode.com (65.49.10.218)
17  206.52 ms scanme.nmap.org (74.207.244.221)

OS and Service detection performed. Please report any incorrect results
at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.89 seconds
root@kali:~#
```

Χωρίς αμφιβολία, η πλέον ενδιαφέρουσα επιλογή που ενεργοποιεί η -A είναι εκείνη για το script scanning. Συνεχίστε το διάβασμα.

Τα πολύτιμα scripts

Το nmap έχει ικανότητες για εκτέλεση scripts, μέσω της σχετικής μηχανής που ενσωματώνει. Πρόκειται για τη λεγόμενη Nmap Scripting Engine (NSE), η οποία διερμηνεύει scripts γραμμένα στη γλώσσα Lua (http://lua.org). Αρχικά τα scripts του nmap προορίζονταν για εργασίες όπως network discovery, προχωρημένο version detection κι ανίχνευση ευπαθειών (vulnerabilities ή αλλιώς vulns). Σήμερα ο βιότοπος των NSE scripts έχει επεκταθεί σημαντικά. Αρκεί ν' αναλογιστούμε ότι μόνο τα επίσημα scripts εμπίπτουν στις ακόλουθες 13 κατηγορίες: auth, broadcast, default, discovery, dos, exploit, external, fuzzer, intrusive, malware, safe, version και vuln.

Πριν αρχίσουμε να παίζουμε με τα NSE scripts, αξίζει να υπογραμμίσουμε ότι δεν εκτελούνται εντός κάποιου προστατευμένου περιβάλλοντος (sandbox). Έτσι, δεν είναι απίθανο να προκαλέσουν ζημιά στο σύστημα ή/και να υπονομεύσουν την ασφάλειά του. Αναφερόμαστε βεβαίως στα ανεπίσημα scripts, τα οποία καλό είναι να μη χρησιμοποιούμε αν δεν εμπιστευόμαστε απόλυτα την πηγή ή/και δεν έχουμε εξετάσει τον κώδικά τους.

Νομίζουμε πως ο καλύτερος τρόπος για να κάνουμε την πρώτη μας γνωριμία με τα scripts, αλλά και για ν' αποκτήσουμε μια καλή ιδέα περί των δυνατοτήτων που προσφέρουν στο χρήστη του nmap, είναι μέσα από μερικά παραδείγματα.

Παράδειγμα 1. Υπάρχουν μηχανήματα στο δίκτυο που προσφέρουν υπηρεσίες DHCP; Αν ναι, ποια είναι;

```
root@kali:~# nmap --script broadcast-dhcp-discover
Starting Nmap 6.47 ( http://nmap.org ) at 2014-09-01 07:19 EEST
Pre-scan script results:
| broadcast-dhcp-discover:
|   IP Offered: 10.10.10.167
|   DHCP Message Type: DHCPOFFER
|   Server Identifier: 10.10.10.254
|   IP Address Lease Time: 0 days, 0:05:00
|   Subnet Mask: 255.255.255.0
|   Router: 10.10.10.254
|   Domain Name Server: 10.10.10.254
|_  Domain Name: parabing.net
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 1.22 seconds
root@kali:~#
```

Παράδειγμα 2. Υπάρχουν μηχανήματα στο δίκτυο που τρέχουν το Dropbox;

```
root@kali:~# nmap --script broadcast-dropbox-listener
Starting Nmap 6.47 ( http://nmap.org ) at 2014-09-01 07:22 EEST
```

```
Pre-scan script results:
| broadcast-dropbox-listener:
| displayname  ip           port   version  host_int   namespaces
|_             10.10.10.10  17500  1.8      107032736  684376, 24259886,
36249577, 40213408, 64654762, 98453486, 98453596, 229234128, 273431026,
273709344, 273719352, 588724142
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 17.31 seconds
root@kali:~#
```

Παράδειγμα 3. Το μηχάνημα 10.10.10.162 τρέχει SAMBA. Δεν έχουμε πρόσβαση στα shares, ωστόσο μπορούμε να δοκιμάσουμε την τύχη μας εξαπολύοντας μια επίθεση brute force:

```
root@kali:~# nmap --script smb-brute -p445 10.10.10.162
Starting Nmap 6.47 ( http://nmap.org ) at 2014-09-01 08:11 EEST
Nmap scan report for 10.10.10.162
Host is up (0.00056s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:EC:48:E4 (Cadmus Computer Systems)
Host script results:
| smb-brute:
|   msfadmin:msfadmin => Valid credentials
|_  user:user => Valid credentials
Nmap done: 1 IP address (1 host up) scanned in 200.76 seconds
root@kali:~#
```

Παράδειγμα 4. Διάφορα μηχανήματα στο τοπικό δίκτυο τρέχουν υπηρεσίες file sharing. Δεν είναι κακή ιδέα να ελέγξουμε για γνωστές αδυναμίες που αφορούν στις αντίστοιχες υπηρεσίες:

```
root@kali:~# nmap --script smb-check-vulns --script-args unsafe=1 -p445
10.10.10.0/24
...
Nmap scan report for JoePC.parabing.net (10.10.10.164)
Host is up (0.0022s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:79:37:C5 (Cadmus Computer Systems)
```

```
Host script results:
| smb-check-vulns:
|   Conficker: Likely CLEAN; access was denied.
|   |  If you have a login, try using --script-
       args=smbuser=xxx,smbpass=yyy
|   |  (replace xxx and yyy with your username and password). Also try
|   |_ smbdomain=zzz if you know the domain. (Error NT_STATUS_ACCESS_
       DENIED)
|   SMBv2 DoS (CVE-2009-3103): NOT VULNERABLE
|   MS06-025: NO SERVICE (the Ras RPC service is inactive)
|_  MS07-029: NO SERVICE (the Dns Server RPC service is inactive)
...
Nmap scan report for secdesk.parabing.net (10.10.10.165)
Host is up (0.0020s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:67:0E:3D (Cadmus Computer Systems)
Host script results:
| smb-check-vulns:
|   MS08-067: LIKELY VULNERABLE (host stopped responding)
|   Conficker: Likely CLEAN
|   SMBv2 DoS (CVE-2009-3103): NOT VULNERABLE
|   MS06-025: NO SERVICE (the Ras RPC service is inactive)
|_  MS07-029: NO SERVICE (the Dns Server RPC service is inactive)
...
root@kali:~#
```

Παράδειγμα 5. Υπάρχει ένα μηχάνημα στο δίκτυο, το 10.10.10.162, το οποίο δείχνει εντελώς απροστάτευτο. Με βάση την πληθώρα των υπηρεσιών που τρέχει, είναι πολύ πιθανό να 'χει κι αδυναμίες πέρα από τις εύκολα αναγνωρίσιμες. Ας κάνουμε πρώτα ένα port scan, ελέγχοντας τις 2000 πιο δημοφιλείς θύρες (εξ ορισμού ελέγχονται οι 1000 πιο δημοφιλείς):

```
root@kali:~# nmap -sV --top-ports 2000 10.10.10.162
Starting Nmap 6.47 ( http://nmap.org ) at 2014-09-01 10:10 EEST
Nmap scan report for 10.10.10.162
Host is up (0.00060s latency).
Not shown: 1976 closed ports
```

```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
...
3632/tcp open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
...
6667/tcp open  irc         Unreal ircd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
...
Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 78.32 seconds
root@kali:~#
```

Εστιάζουμε την προσοχή μας στις υπηρεσίες ονόματι distccd και ircd. Ξεκινάμε με την πρώτη:

```
root@kali:~# nmap --script distcc* -p 3632 10.10.10.162
Starting Nmap 6.47 ( http://nmap.org ) at 2014-09-01 10:17 EEST
Nmap scan report for 10.10.10.162
Host is up (0.00054s latency).
PORT     STATE SERVICE
3632/tcp open  distccd
| distcc-cve2004-2687:
|   VULNERABLE:
|   distcc Daemon Command Execution
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2004-2687
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|     Description:
|       Allows executing of arbitrary commands on systems running
        distccd 3.1 and
|       earlier. The vulnerability is the consequence of weak service
        configuration.
|
|     Disclosure date: 2002-02-01
```

```
 |     Extra information:
 |
 |     uid=1(daemon) gid=1(daemon) groups=1(daemon)
 |
 |     References:
 |       http://http://www.osvdb.org/13378
 |       http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2687
 |       http://distcc.googlecode.com/svn/trunk/doc/web/security.html
 |_      http://http://web.nvd.nist.gov/view/vuln/
         detail?vulnId=CVE-2004-2687
MAC Address: 08:00:27:EC:48:E4 (Cadmus Computer Systems)
Nmap done: 1 IP address (1 host up) scanned in 13.52 seconds
root@kali:~#
```

Σημειώστε ότι το πλήρες όνομα του script που μόλις χρησιμοποιήσαμε είναι "distcc-cve2004-2687". Το nmap όμως δεν μας υποχρεώνει να θυμόμαστε τα ονόματα των scripts. Γι' αυτό κι εμείς απλά γράψαμε "distcc" και μετά έναν αστερίσκο (χαρακτήρας-μπαλαντέρ). Σ' αυτές τις περιπτώσεις, το nmap ψάχνει για scripts που να ταιριάζουν στο μοτίβο που έχει ορίσει ο χρήστης. Αν βρει κάποια, τα εκτελεί. (Στο παράδειγμα με την υπηρεσία distcc, υπάρχει ακριβώς ένα script.) Σειρά τώρα έχει η υπηρεσία ircd:

```
root@kali:~# nmap --script irc*unreal* -p 6667 10.10.10.162
Starting Nmap 6.47 ( http://nmap.org ) at 2014-09-01 10:46 EEST
Nmap scan report for 10.10.10.162
Host is up (0.0013s latency).
PORT     STATE SERVICE
6667/tcp open  irc
|_irc-unrealircd-backdoor: Looks like trojaned version of unrealircd.
  See http://seclists.org/fulldisclosure/2010/Jun/277
MAC Address: 08:00:27:EC:48:E4 (Cadmus Computer Systems)
Nmap done: 1 IP address (1 host up) scanned in 21.39 seconds
root@kali:~#
```

Παράδειγμα 6. Προσφάτως διαβάσαμε ότι, παρά τη μεγάλη έκταση που είχε πάρει η ιστορία με το Heartbleed bug (βλ. σχετικό άρθρο στο deltaHacker 031, http://deltahacker.gr/?p=11543), υπάρχει ένα σημαντικό ποσοστό servers Εκεί Έξω (TM) οι οποίοι παραμένουν unpatched. Χάρη στο script ονόματι ssl-heartbleed είναι εύκολο να εντοπίσουμε τέτοια μηχανήματα. (Το πώς ακριβώς δεν σας το λέμε, αν όμως διαβάσετε προσεκτικά το άρθρο της σελίδας 24 θα το καταλάβετε πανεύκολα.) Ιδού τα αποτελέσματα της εκτέλεσης του ssl-heartbleed, σε ένα ευπαθές μηχάνημα κάπου στο Internet:

```
root@kali:~# nmap --script ssl-heartbleed -p 443 xxxyyyzzz.alshamil.abc.ae
Starting Nmap 6.47 ( http://nmap.org ) at 2014-09-01 09:19 EEST
Nmap scan report for xxxyyyzzz.alshamil.abc.ae (217.p.q.r)
Host is up (0.17s latency).
PORT    STATE SERVICE
443/tcp open  https
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL
    cryptographic software library. It allows for stealing information
    intended to be protected by SSL/TLS encryption.
|     State: VULNERABLE
|     Risk factor: High
|     Description:
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f
        and 1.0.2-beta1) of OpenSSL are affected by the Heartbleed
        bug. The bug allows for reading memory of systems protected by
        the vulnerable OpenSSL versions and could allow for disclosure
        of otherwise encrypted confidential information as well as the
        encryption keys themselves.
|
|     References:
|       http://cvedetails.com/cve/2014-0160/
|       http://www.openssl.org/news/secadv_20140407.txt
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
Nmap done: 1 IP address (1 host up) scanned in 1.84 seconds
root@kali:~#
```

Αλήθεια, πού στον πλανήτη είναι αυτός ο —μάλλον ξεχασμένος— server; Υπάρχουν ορισμένα scripts του nmap, με χρήση των οποίων είναι δυνατόν να παίρνουμε χρήσιμες απαντήσεις σε παρόμοια ερωτήματα:

```
root@kali:~# nmap --script ip-geolocation-* xxxyyyzzz.alshamil.abc.ae
Starting Nmap 6.47 ( http://nmap.org ) at 2014-09-01 09:23 EEST
Nmap scan report for xxxyyyzzz.alshamil.abc.ae (217.p.q.r)
Host is up (0.18s latency).
Not shown: 996 filtered ports
PORT     STATE   SERVICE
```

```
113/tcp  closed ident
443/tcp  open   https
8000/tcp closed http-alt
8009/tcp open   ajp13
Host script results:
| ip-geolocation-geobytes:
|   latitude: 25.23
|   longitude: 55.28
|   city: Dubai
|   region: Dubayy
|_  country: United Arab Emirates
| ip-geolocation-geoplugin:
| 217.p.q.r (xxxyyyzzz.alshamil.abc.ae)
|   coordinates (lat,lon): 24.4667,54.366699
|_  state: Ab\xC5\xAB Z\xCC\xA7aby, United Arab Emirates
|_ip-geolocation-maxmind: ERROR: Script execution failed (use -d to
  debug)
Nmap done: 1 IP address (1 host up) scanned in 12.04 seconds
root@kali:~#
```

Χρήση των scripts

Όπως έγινε φανερό στα προηγούμενα παραδείγματα, προκειμένου να εκτελέσουμε ένα script δίνουμε κάτι σαν

```
nmap --script όνομα_script στόχος
```

ή, ισοδύναμα, κάτι σαν

```
nmap --script=όνομα_script στόχος
```

(Η διαφορά στις δύο γραμμές είναι στην απουσία ή όχι του "ίσον", στα δεξιά του "--script".) Γενικότερα, στη θέση του όνομα_script μπορούμε να βάζουμε μια λίστα με ονόματα scripts ή/και ονόματα καταλόγων (οι οποίοι περιλαμβάνουν scripts) ή/και κατηγορίες scripts. Τα στοιχεία της λίστας χωρίζονται με κόμματα.

Να σημειώσουμε εδώ ότι η δημοφιλής επιλογή -A εμπεριέχει την -sC, η οποία με τη σειρά της σημαίνει "--script default", δηλαδή εκτέλεση *όλων* των scripts που ανήκουν στην κατηγορία default. Αν, π.χ., σκανάρουμε το VM με το Metasploitable (10.10.10.162) πληκτρολογώντας

```
root@kali:~# nmap --script default 10.10.10.162
```

τότε θα εκτελεστούν όλα τα scripts της κατηγορίας default. Μεταξύ αυτών είναι και το script ονόματι ssh-hostkey, το οποίο επιστρέφει το δημόσιο ή τα δημόσια κλειδιά ενός SSH server. Όποτε ψάχνουμε για μία συγκεκριμένη πληροφορία, καλό είναι να σκανάρουμε πιο στοχευμένα. Παράδειγμα:

```
root@kali:~# nmap --script ssh-hostkey -p 22 10.10.10.162
Starting Nmap 6.47 ( http://nmap.org ) at 2014-09-01 13:06 EEST
Nmap scan report for 10.10.10.162
Host is up (0.00047s latency).
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
MAC Address: 08:00:27:EC:48:E4 (Cadmus Computer Systems)
Nmap done: 1 IP address (1 host up) scanned in 13.47 seconds
root@kali:~#
```

Η δε επιλογή --script-help δέχεται ως παράμετρο μια λίστα με ονόματα scripts, καταλόγων ή κατηγοριών, και κάνει αυτό που υποδηλώνει το όνομά της. Δείτε:

```
root@kali:~# nmap --script-help ssh-hostkey
Starting Nmap 6.47 ( http://nmap.org ) at 2014-09-01 13:19 EEST
ssh-hostkey
Categories: safe default discovery
http://nmap.org/nsedoc/scripts/ssh-hostkey.html
  Shows SSH hostkeys.
  Shows the target SSH server's key fingerprint and (with high enough
  verbosity level) the public key itself.  It records the discovered host keys
  in <code>nmap.registry</code> for use by other scripts.  Output can be
  controlled with the <code>ssh_hostkey</code> script argument.
  You may also compare the retrieved key with the keys in your known-hosts
  file using the <code>known-hosts</code> argument.
  The script also includes a postrule that check for duplicate hosts using the
  gathered keys.
root@kali:~#
```

Να κι άλλο ένα παράδειγμα, όπου παίρνουμε βοήθεια για *όλα* τα scripts της κατηγορίας ονόματι "dos" (Denial of Service):

```
root@kali:~# nmap --script-help dos|less
```

(Πατήστε το [Q] για να βγείτε από το less.) Δοκιμάστε τώρα να πληκτρολογήσετε αυτό:

```
root@kali:~# nmap --script-help all|less
```

Θα πάρετε μια μακροσκελή λίστα με όλα τα διαθέσιμα scripts, αλφαβητικά ταξινομημένα. Ίσως έχετε ήδη παρατηρήσει ότι ένα script επιτρέπεται να ανήκει σε περισσότερες από μία κατηγορίες. Πολύ εύκολα, μπορούμε να ζητάμε την εκτέλεση scripts που ανήκουν σε τουλάχιστον μία κατηγορία από ένα σύνολο προκαθορισμένων. Εναλλακτικά, έχουμε τη δυνατότητα εκτέλεσης scripts που ανήκουν σε δύο ή περισσότερες κατηγορίες ταυτόχρονα. Κι επειδή φανταζόμαστε ότι δεν είναι όλοι οι αναγνώστες του περιοδικού εξεικοιωμένοι με τη Μαθηματική Θεωρία Συνόλων, ας προσέξουμε τα παραδείγματα που ακολουθούν.

Γράφοντας κάτι σαν

```
nmap --script "default or safe" the_target
```

λέμε στο nmap να σκανάρει το στόχο the_target τρέχοντας όλα τα scripts που ανήκουν στην κατηγορία default ή στην κατηγορία safe ή και στις δύο ταυτόχρονα. Από την άλλη, πληκτρολογώντας κάτι σαν

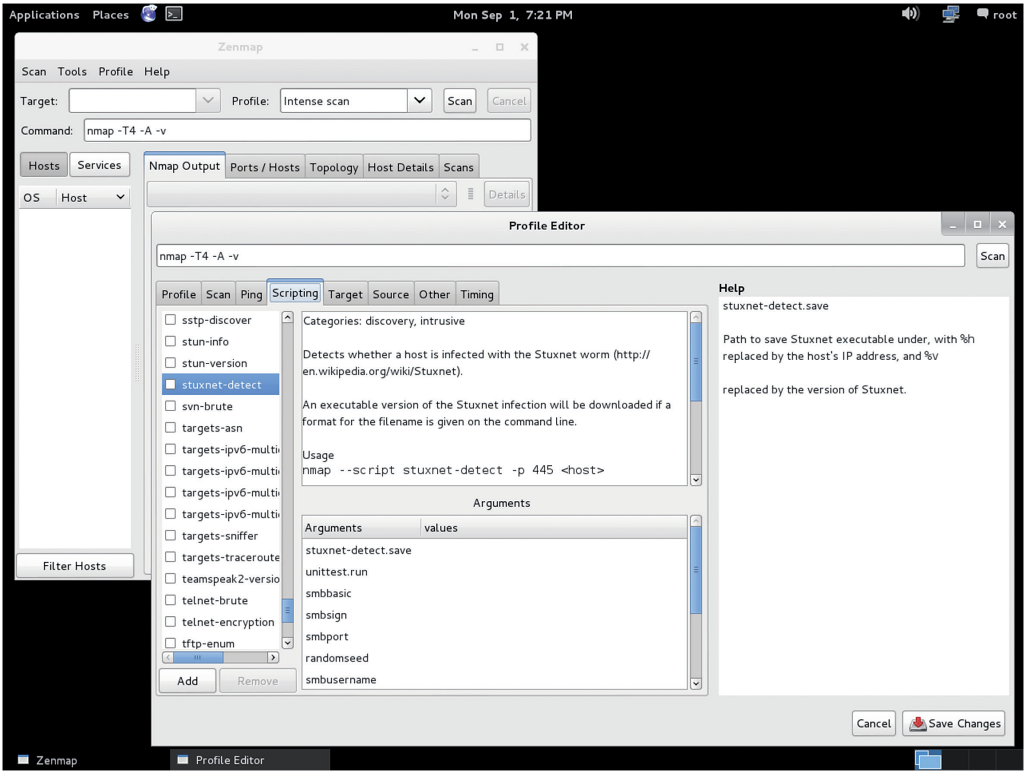
```
nmap --script "default and safe" the_target
```

σκανάρουμε τον στόχο the_target ενεργοποιώντας τα scripts που ανήκουν στις κατηγορίες default και safe ταυτόχρονα. Η --script καταλαβαίνει τον τελεστή της άρνησης (not) και λαμβάνει υπόψη τις παρενθέσεις, επομένως έχουμε τεράστια ευελιξία ως προς την επιλογή scripts προς εκτέλεση. Δείτε:

```
nmap --script "(intrusive or exploit or vuln or dos) and not mysql*"
```

Τέλος, όπως θα παρατηρήσατε και στο παράδειγμα 4 της προηγούμενης ενότητας, τα scripts επιδέχονται παραμέτρους με τη βοήθεια της επιλογής --script-args. Παροτρύνεστε να πειραματιστείτε με την ησυχία σας με τα NSE scripts, στο δικό σας (εικονικό) εργαστήριο. Θα διαπιστώσετε ότι η σχετική τεκμηρίωση που παρέχεται από τον επίσημο δικτυακό τόπο του nmap (http://nmap.org/book/nse) είναι ποιοτική κι εξαιρετικά χρήσιμη. Για όλες τις κατηγορίες των scripts πηγαίνετε απευθείας στο http://nmap.org/book/nse-usage.html#nse-categories, ενώ για γρήγορη πρόσβαση στις κατηγορίες ή/και σε μεμονωμένα scripts δείτε το http://nmap.org/nsedoc. Εναλλακτικά, εξετάστε όλα τα διαθέσιμα scripts, διαβάστε τι κάνει το καθένα αλλά δείτε και πολύτιμα παραδείγματα χρήσης, μέσα από το περιβάλλον του Zenmap: Επιλέξτε Profile → New Profile or Command και στο νέο παράθυρο που θα εμφανιστεί κάντε κλικ στην καρτέλα "Scripting".

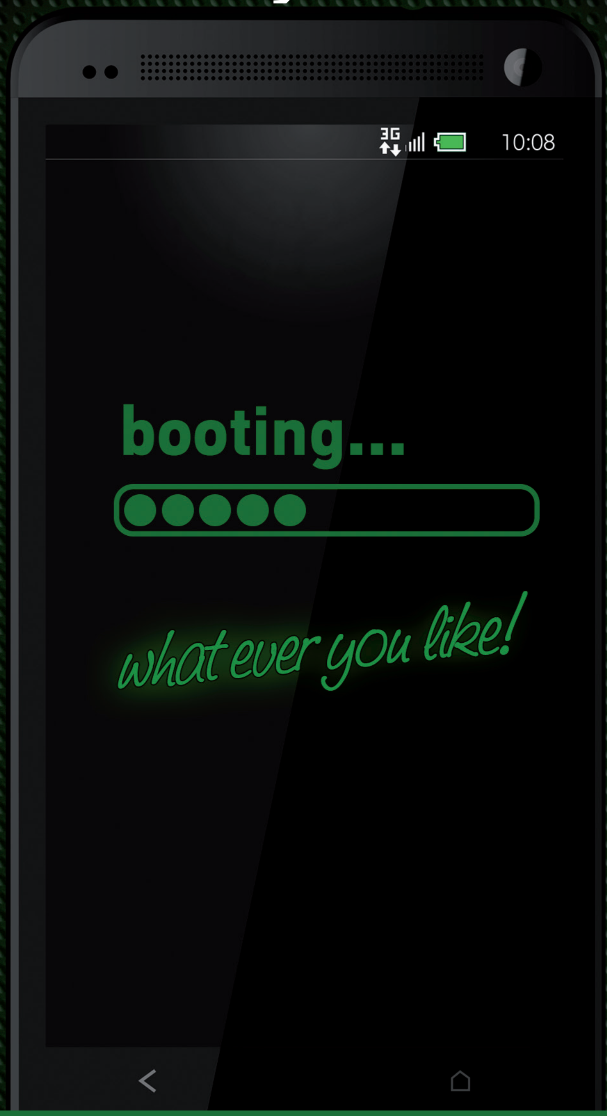
Βάζουμε εδώ μια άνω τελεία, να σας αφήσουμε κι εσάς να παίξετε με την ησυχία σας. Επιφυλασσόμεθα να επανέλθουμε σύντομα στο nmap, με περισσότερα σενάρια χρήσης και πρακτικές εφαρμογές. Προς το παρόν έχουμε κατά νου κάποια άρθρα, τα οποία κατά πάσα πιθανότητα θα δημοσιεύσουμε στο site του περιοδικού. Έως τότε, καλή σας διασκέδαση!



Από το φιλικό περιβάλλον του Zenmap έχουμε την ευκαιρία να εξετάσουμε άνετα όλα τα διαθέσιμα NSE scripts, να μάθουμε λεπτομέρειες για την αποστολή τους αλλά και να δούμε πώς ακριβώς τα χρησιμοποιούμε στα δικά μας scans.

Skill: Beginner
Tags: Android, boot, root, animation

by multiPetros



Βάλτε τη δική σας σφραγίδα στο Android!

Το δημοφιλές λειτουργικό σύστημα της Google μάς έχει απασχολήσει πολλές φορές. Έχουμε εξετάσει διάφορες λειτουργίες του κι έχουμε σκαλίσει αρκετές ρυθμίσεις – φανερές και κρυφές. Αυτή τη φορά, υπό την επήρεια του καύσωνα θα ασχοληθούμε με κάτι ανάλαφρο. Δεν θα προσπαθήσουμε να επέμβουμε στη λειτουργικότητα του συστήματος, αλλά στην αισθητική του. Συγκριμένα, θα καταστήσουμε την οθόνη έναρξης μοναδική και απόλυτα προσωποποιημένη!

Το Android αποτελεί την αγαπημένη επιλογή των απανταχού κατασκευαστών φορητών συσκευών. Πέρα από το μηδενικό κόστος, ο ανοιχτός χαρακτήρας του Android επιτρέπει την εύκολη παραμετροποίηση της λειτουργικότητας αλλά και της όψης του συστήματος. Έτσι, πολλοί κατασκευαστές αναπτύσσουν τα δικά τους app launchers, τα εγκαθιστούν στις συσκευές τους και μ' αυτόν τον τρόπο καταφέρνουν να διαφοροποιούν τα προϊόντα τους από τα υπόλοιπα. Ορισμένες φορές οι σχετικές επεμβάσεις είναι τόσο βαθιές κι εκτεταμένες, που οι αντίστοιχες συσκευές συγκροτούν ένα ξεχωριστό οικοσύστημα. Πάντως, ακόμα κι όσοι δεν καταπιάνονται σ' αυτό το βαθμό με την παραμετροποίηση του Android, είναι σίγουρο ότι φροντίζουν ν' αφήσουν το στίγμα τους μ' έναν απλούστερο τρόπο: Τοποθετούν το λογότυπό τους —μια στατική εικόνα ή ακόμα κι ένα σύντομο animation— στην οθόνη έναρξης του συστήματος. Ε, λοιπόν, κάτι παρόμοιο σκοπεύουμε να κάνουμε κι εμείς! Δεν θα ήταν ωραίο να βλέπουμε ένα σηματάκι της δικής μας επιλογής, κάθε φορά που ενεργοποιούμε την αγαπημένη μας συσκευή; Το μόνο που έχουμε να κάνουμε είναι να ακολουθήσουμε μερικά απλά βήματα.



Οι συσκευές με Android διαθέτουν συνήθως διαφορετικά boot animations, εμφανίζοντας κάθε φορά το λογότυπο του αντίστοιχου κατασκευαστή.

Εν αρχή ην ο root

Το πρώτο βήμα που πρέπει να κάνουμε —αν δεν το έχουμε κάνει ήδη— πριν καταπιαστούμε με εικόνες ή και με μικρά animations, είναι το λεγόμενο rooting. Ως γνωστόν, το rooting αποτελεί τη διαδικασία με την οποία αποκτάμε πρόσβαση στο λειτουργικό σύστημα της συσκευής, με τα δικαιώματα του χρήστη root. Με αυτόν τον τρόπο μπορούμε να πραγματοποιούμε ενέργειες που υπό φυσιολογικές συνθήκες θα ήταν απαγορευμένες. Για παράδειγμα, μπορούμε να τροποποιήσουμε αρχεία του λειτουργικού συστήματος, να αφαιρέσουμε προεγκατεστημένες εφαρμογές κ.ο.κ. Η διαδικασία του rooting διαφέρει από συσκευή σε συσκευή. Παρ' όλα αυτά, μια ανάγνωση του σχετικού άρθρου που δημοσιεύτηκε στο τεύχος 004 του deltaHacker, καθώς και μια περαιτέρω αναζήτηση στο forum των xda developers, είναι σίγουρο ότι θα σας βοηθήσουν να πετύχετε το rooting της συσκευής σας πολύ γρήγορα. Φυσικά, υπάρχουν κι εργαλεία που αυτοματοποιούν το rooting, αλλά δεν υποστηρίζουν όλες τις συσκευές. Ένα γνωστό εργαλείο της κατηγορίας, που υποστηρίζει και μια μεγάλη γκάμα συσκευών, είναι το vRoot. Μπορείτε να το κατεβάσετε από τη διεύθυνση www.mgyun.com/en/getvroot.

File manager χωρίς σύνορα

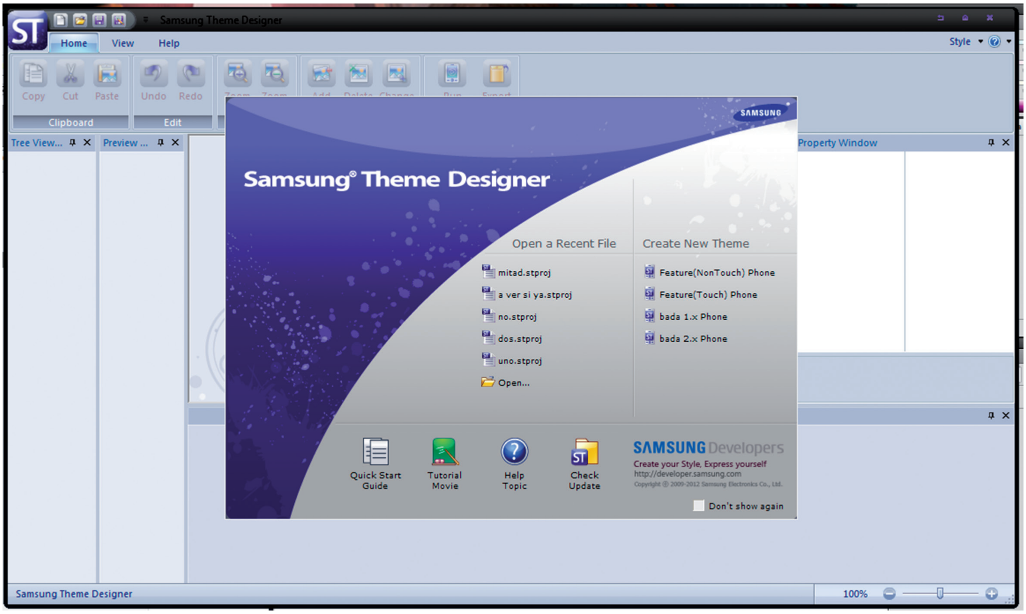
Δεύτερο βήμα αποτελεί η εγκατάσταση στη συσκευή μας ενός file manager. Μπορούμε να προσθέσουμε οποιονδήποτε μας αρέσει, με μόνη προϋπόθεση να παρέχει πρόσβαση στη ρίζα του συστήματος αρχείων (/) και όχι μόνο στο /mnt, το οποίο περιλαμβάνει συνήθως τον "εσωτερικό" αποθηκευτικό χώρο της συσκευής και την κάρτα μνήμης. Μια πολύ καλή επιλογή αποτελεί ο ZArchiver, ο οποίος μάλιστα μπορεί να συμπιέζει και να αποσυμπιέζει αρχεία ZIP και 7zip. Μερικές ακόμα καλές επιλογές συνιστούν οι ES File Explorer, ASTRO File Manager, Total Commander κ.ά., που πραγματοποιούν όλες τις εργασίες που χρειαζόμαστε για το εγχείρημά μας. Η επιλογή κάποιου από αυτούς εναπόκειται κυρίως στο προσωπικό γούστο του καθενός. Αν η συσκευή σας διαθέτει μόνο τον τεχνητά περιορισμένο stock file manager, αρκεί μια βόλτα από το πλησιέστερο marketplace, όπου και θα βρούμε αρκετές υλοποιήσεις και μάλιστα δωρεάν.

Ακτινογραφία του boot animation

Το αρχείο που είναι υπεύθυνο για το boot animation ονομάζεται bootanimation.zip και θα το βρούμε στον κατάλογο /system/media (σε ορισμένες ROM βρίσκεται στη θέση /data/local, ενώ στις συσκευές HTC βρίσκεται στη θέση /system/customize/resource). Αν εξετάσουμε το περιεχόμενο του bootanimation.zip της συσκευής μας, θα διαπιστώσουμε ότι περιέχει ένα αρχείο κειμένου με το όνομα desc.txt κι έναν ή περισσότερους φακέλους με ονόματα part0, part1 κ.ο.κ. Μέσα σε αυτούς τους φακέλους φιλοξενούνται εικόνες PNG ή JPG, με κατάλληλα ονόματα που περιλαμβάνουν αριθμούς. Περισσότερα γι' αυτά τα ονόματα θα πούμε σε λίγο. Αν οπτικοποιούσαμε τη διάρθρωση του bootanimation.zip με τη βοήθεια του ASCII art, θα βλέπαμε κάτι τέτοιο:

```
bootanimation.zip
|-- desc.txt
|-- part0
    |-- img001.png
    |-- img002.png
    |-- img003.png
|-- part1
    |-- img004.png
    |-- img005.png
    |-- img006.png
    |-- img007.png
```

Ας μελετήσουμε τώρα τα αρχεία που περιλαμβάνει ένα τυπικό bootanimation.zip, ξεκινώντας από το desc.txt. Όπως πολύ σωστά φαντάζεστε, το συγκεκριμένο αρχείο περιέχει όλες τις πληροφορίες για την αναπαραγωγή του animation. Στην πρώτη γραμμή του desc.txt ορίζεται το πλάτος και το ύψος του animation σε pixels, καθώς και το framerate (σε πλήθος καρέ ανά δευτερόλεπτο). Αυτά τα τρία μεγέθη δεν συνοδεύονται από κάποια μονάδα και χωρίζονται μεταξύ τους με ένα κενό. Οι επόμενες γραμμές του desc.txt ξεκινούν με το γράμμα "p" και περιγράφουν τα ξεχωριστά τμήματα που απαρτίζουν το animation. Μετά από το "p" συναντάμε πάντα δύο αριθ-



Η εφαρμογή Samsung Theme Designer είναι απαραίτητη για τη δημιουργία ενός boot animation, για τις συσκευές της Samsung.

μούς: Ο πρώτος δηλώνει πόσες φορές θα επαναληφθεί το συγκεκριμένο τμήμα του animation (εδώ η τιμή 0 σημαίνει άπειρες επαναλήψεις), ενώ ο δεύτερος αριθμός προσδιορίζει την παύση (τη χρονική καθυστέρηση) κατά τη μετάβαση στο επόμενο τμήμα του animation. Οι γραμμές που ξεκινούν με το "p" ολοκληρώνονται με το όνομα του φακέλου που περιλαμβάνει τα καρέ του αντίστοιχου τμήματος του animation. Σε αυτές τις γραμμές, οι διάφορες τιμές χωρίζονται και πάλι με τον χαρακτήρα του κενού. Ας δούμε τώρα κι ένα απλό παράδειγμα, για να κατανοήσουμε καλύτερα όσα περιγράψαμε προηγουμένως.

```
512 256 30
p 1 0 part0
p 0 0 part1
```

Τα παραπάνω μεταφράζονται ως εξής: Το animation έχει πλάτος 512 pixels και ύψος 256 pixels, ενώ ο ρυθμός αναπαραγωγής ανέρχεται στα 30 καρέ ανά δευτερόλεπτο. Το animation αποτελείται από δύο τμήματα: Το πρώτο θα επαναληφθεί μια φορά κι αμέσως μετά θα ξεκινήσει το επόμενο, χωρίς καμία καθυστέρηση. Οι εικόνες του πρώτου τμήματος βρίσκονται στον κατάλογο part0. Το δεύτερο τμήμα του animation θα εκτελείται επ' άπειρον (πρακτικά, έως ότου ολοκληρωθεί το boot της συσκευής) και στο τέλος δεν θα προστεθεί καμία καθυστέρηση. Οι εικόνες που το απαρτίζουν βρίσκονται στον κατάλογο part1.

Απλό δεν ήταν; Ας εξετάσουμε τώρα και τις εικόνες (τα καρέ) που απαρτίζουν τα διάφορα τμήματα του animation. Αυτές πρέπει να είναι αποθηκευμένες σε φορμά PNG ή JPG, με χρωματικό προφίλ RGB και βάθος χρώματος στα 24bit[1]. Φυσικά, το μέγεθός τους πρέπει να είναι ίδιο με εκείνο που έχει δηλωθεί και στο desc.txt, για

1. Σημειώστε ότι τα αρχεία PNG *δεν* πρέπει να είναι interlaced.

ολόκληρο το animation. Τα ονόματα των αρχείων χρειάζονται λίγη προσοχή. Η σειρά τους, αν ταξινομηθούν αλφαβητικά και κατά αύξουσα σειρά, αντιστοιχεί στη σειρά με την οποία θα εμφανίζονται οι αντίστοιχες εικόνες. Ακριβώς γι' αυτό, τα ονόματα περιλαμβάνουν συνήθως και αριθμητικές τιμές, που καθιστούν την ταξινόμηση εύκολη. Οι αριθμοί που χρησιμοποιούνται στα ονόματα έχουν σταθερό μήκος κι αυτό επιτυγχάνεται με την προσθήκη του κατάλληλου πλήθους μηδενικών στα αριστερά. Με αυτόν τον τρόπο αποφεύγονται ορισμένα ύπουλα σφάλματα στην ταξινόμηση. Για να κατανοήσετε σε ποιου είδους σφάλματα αναφερόμαστε, υποθέστε ότι έχουμε δύο εικόνες με τα ονόματα img10.png και img2.png. Αν ταξινομήσουμε αλφαβητικά αυτά τα ονόματα, το img10.png έρχεται πρώτο, επειδή ο χαρακτήρας 1 προηγείται του χαρακτήρα 2. Υποθέστε τώρα ότι έχουμε εφαρμόσει το κολπάκι με τα μηδενικά. Σε αυτή την περίπτωση τα ονόματα των αρχείων θα έχουν αλλάξει σε img10.png και img02.png ή img010.png και και img002.png και πάει λέγοντας. Αν τα ταξινομήσουμε τώρα, το img02.png θα προηγηθεί του img10.png. Επομένως, οι εικόνες θα εμφανιστούν ακριβώς με τη σειρά που επιθυμούμε.

Τέλος, πρέπει να σημειώσουμε ότι το πακέτο bootanimation.zip απαιτεί *μηδενικό* επίπεδο συμπίεσης. Στα περισσότερα προγράμματα συμπίεσης, η σχετική επιλογή αναφέρεται ως "archive only[2]".

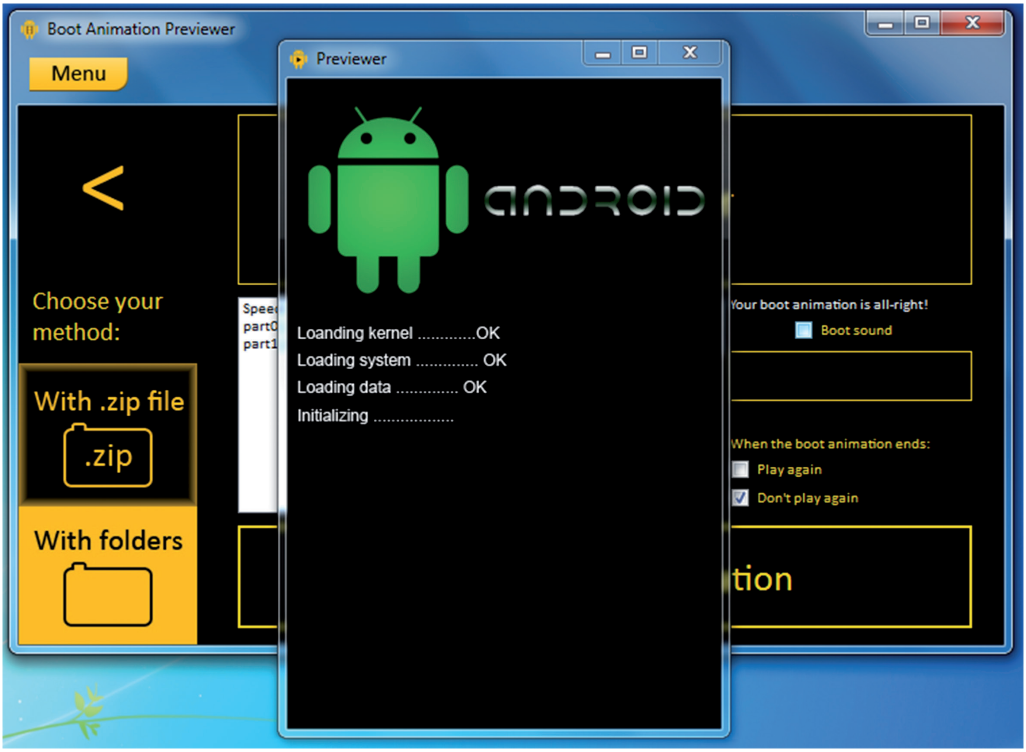
Μια ιδιαίτερη περίπτωση

Όπως είπαμε και νωρίτερα, ορισμένοι κατασκευαστές πραγματοποιούν εκτεταμένες επεμβάσεις στον κώδικα του Android, για διάφορους λόγους. Έτσι, η Samsung έχει επέμβει στον τρόπο λειτουργίας του boot animation, με σκοπό να πετύχει τη συμβατότητα με τα boot animations των παλαιότερων συσκευών της (feature phones). Οι εκδοχές του Android που διαθέτουν οι συσκευές της Samsung δεν χρησιμοποιούν το αρχείο bootanimation.zip. Αντί αυτού διαθέτουν τα αρχεία bootsamsung.qmg και bootsamsungloop.qmg. Ωστόσο, τα δύο αρχεία βρίσκονται εκεί όπου θα περιμέναμε να συναντήσουμε το bootanimation.zip (/system/media). Το πρώτο αρχείο περιέχει τα καρέ από το τμήμα του animation που *δεν* επαναλαμβάνεται, ενώ το δεύτερο αρχείο περιλαμβάνει τα καρέ από το επαναλαμβανόμενο τμήμα του animation. Κατά κάποιον τρόπο, το bootsamsung.qmg αντιστοιχεί στο τμήμα part0 του παραδείγματος που εξετάσαμε προηγουμένως και το bootsamsungloop.qmg αντιστοιχεί στο τμήμα part1. Τα αρχεία QMG, σε αντίθεση με το bootanimation.zip, δεν αποσυμπιέζονται και είναι επεξεργάσιμα με τα κλασικά εργαλεία. Για την επέμβαση στο περιεχόμενό τους απαιτείται το εργαλείο Samsung Theme Designer. Πρόκειται για ένα πρόγραμμα που διανέμεται από την εταιρεία δωρεάν και το οποίο μπορούμε να κατεβάσουμε από τη διεύθυνση `http://developer.samsung.com/themes/tools-sdks/Samsung-Theme-Designer-2-0-4`.

Όπως καταλαβαίνετε, το Samsung Theme Designer αποτελεί ένα εργαλείο για τη δημιουργία ολόκληρων θεμάτων (themes) και όχι μόνο ενός animation. Ωστόσο, κανείς δεν μας εμποδίζει να φτιάξουμε δύο απλοϊκά θέματα, εστιάζοντας κάθε φορά στο animation και μόνο. Στη συνέχεια, μπορούμε να αποσυμπιέσουμε το πακέτο που παράγει η εφαρμογή για κάθε θέμα κι από εκεί να αντιγράψουμε τα αρχεία που αντιστοιχούν στα δύο animations. Ας δούμε τη σχετική διαδικασία επί τροχάδην...

Αφού εγκαταστήσουμε το Samsung Theme Designer, το εκτελούμε κι επιλέγουμε τη δημιουργία ενός θέματος για "Feature(Non Touch) phone". Κατόπιν διαλέγουμε ένα οποιοδήποτε μοντέλο (δεν έχει καμία σημασία ποιο), δίνουμε ένα επιθυμητό όνομα

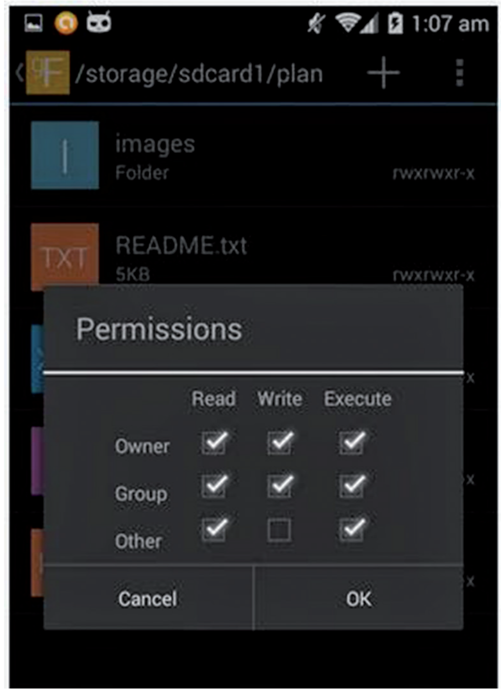
2. Ή "μόνο για αρχειοθέτηση", επί το ελληνικότερον.



Με τη βοήθεια του Boot Animation Previewer μπορούμε να ελέγξουμε το αποτέλεσμα της δουλειάς μας, πριν επέμβουμε στα αρχεία συστήματος της συσκευής!

για το θέμα (theme) και προχωράμε. Στο "Tree view window", που εμφανίζεται στα αριστερά, επιλέγουμε το "Idle component" κι εν συνεχεία το "Idle background", που εμφανίζεται λίγο χαμηλότερα. Από την καρτέλα ιδιοτήτων που εμφανίζεται στη δεξιά πλευρά του προγράμματος, κάνουμε κλικ στην ιδιότητα "Background Type" κι επιλέγουμε "Animated", ενώ στην ιδιότητα "Repeat" επιλέγουμε την τιμή "False". Όπως υποψιάζεστε, σκοπεύουμε να δημιουργήσουμε το πρώτο τμήμα του boot animation, τα οποίο δεν θα επαναλαμβάνεται. Στην ιδιότητα "Frame" ορίζουμε τον πλήθος των καρέ, ενώ αμέσως από κάτω στην ιδιότητα "Duration" εισάγουμε την επιθυμητή διάρκεια εμφάνισης του κάθε καρέ σε milliseconds. Για να μεταφράσουμε τη διάρκεια αυτή σε καρέ ανά δευτερόλεπτο (FPS) πρέπει να διαιρέσουμε το 1000 με το επιθυμητό FPS. Για παράδειγμα, για 30 καρέ ανά δευτερόλεπτο πρέπει να ορίσουμε Duration = 1000 / 30 ≈ 33 ms. Κάπως έτσι, στην κάτω πλευρά του παραθύρου του προγράμματος θα έχουν εμφανιστεί διάφορα ορθογώνια πλαίσια, καθένα από τα οποία αντιστοιχεί στα καρέ του animation. Τώρα δεν έχουμε παρά να σύρουμε σε κάθε πλαίσιο την επιθυμητή εικόνα. Αφού σχηματίσουμε το animation, μεταβαίνουμε στην περιοχή "Home" του ribbon menu του προγράμματος και κάνουμε κλικ στο "Export theme". Όταν ολοκληρώσουμε την "εξαγωγή" θα έχει δημιουργηθεί ένα αρχείο με την κατάληξη SMT. Ουσιαστικά πρόκειται για ένα πακέτο ZIP και, αν το ανοίξουμε, θα βρούμε στο εσωτερικό του το αρχείο IdleBgAnimObj.qmg. Ε, λοιπόν, αυτό αρχείο αποτελεί το πρώτο τμήμα του boot animation που κατασκευάζουμε. Επομένως, το μετονομάζουμε σε bootsamsung.qmg και το βάζουμε στην άκρη.

Νομίζουμε ότι έχετε πιάσει το κολπάκι μας! Τώρα πρέπει να χρησιμοποιήσουμε πάλι το Samsung Theme Designer, για να κατασκευάσουμε το επαναλαμβανόμενο τμήμα του boot animation. Επομένως, ξεκινάμε τη δημιουργία ενός νέου theme και πραγματοποιούμε τις επιλογές που είδαμε και προηγουμένως. Αυτή τη φορά, όμως, όταν φτάσουμε στην ιδιότητα "Repeat" επιλέγουμε την τιμή "True". Συνεχίζουμε με το γνωστό τρόπο: Σχηματίζουμε το animation, κάνουμε export το θέμα και αποσυμπιέζουμε το αρχείο SMT που προκύπτει. Από εκεί παίρνουμε το αρχείο IdleBgAnimObj.qmg και το μετονομάζουμε σε bootsamsungloop.qmg. Με αυτό το κολπάκι καταφέρνουμε να φτιάξουμε ένα boot animation, συμβατό με την εκδοχή του Android που χρησιμοποιούν οι συσκευές της Samsung!



Πριν προχωρήσουμε στην εγκατάσταση του νέου boot animation, οφείλουμε να τροποποιήσουμε τα δικαιώματα του φακέλου /system/media και, συγκεκριμένα, να προσθέσουμε το δικαίωμα εγγραφής. Κάτι τέτοιο μπορεί να γίνει πανεύκολα από τον file manager.

Τελευταίο στάδιο!

Στην περίπτωση που κατασκευάσαμε ένα boot animation για το stock Android, μπορούμε να το δοκιμάσουμε πριν το τοποθετήσουμε στη συσκευή. Για το σκοπό αυτό προσφέρεται το εργαλείο Boot Animation Previewer, που μπορείτε να κατεβάσετε από το http://bit.ly/dh035bootanimprev. Το συγκεκριμένο πρόγραμμα προορίζεται για συστήματα με Windows και πετυχαίνει την αναπαραγωγή των boot animations με τον ίδιο ακριβώς τρόπο που γίνεται κι από το Android.

Εφόσον έχουμε ολοκληρώσει το rooting της συσκευής μας, έχουμε εγκαταστήσει έναν αξιοπρεπή file manager κι έχουμε ετοιμάσει το νέο boot animation, μπορούμε (επιτέλους) να το εγκαταστήσουμε. Για το σκοπό αυτό ανοίγουμε τον file manager, μεταβαίνουμε στην τοποθεσία /system/media κι εντοπίζουμε το αρχείο bootanimation.zip[3]. Πριν κάνουμε οποιαδήποτε άλλη κίνηση, είναι φρόνιμο να δημιουργήσουμε ένα αντίγραφο του εργοστασιακού boot animation, αντιγράφοντας το αρχείο bootanimation.zip σε κάποιον άλλον κατάλογο (π.χ., κάπου στην κάρτα SD). Στη συνέχεια, μέσα από τον file manager πάντα, αλλάζουμε τα δικαιώματα του φακέλου /system/media από read only σε read/write. Τέλος, αντικαθιστούμε το εργοστασιακό bootanimation.zip με εκείνο που έχουμε δημιουργήσει. Για λόγους ασφαλείας είναι καλό να τροποποιήσουμε ξανά τα δικαιώματα του φακέλου /system/media και να τα επαναφέρουμε στην αρχική τους κατάσταση (read only). Μετά κι απ' αυτό, είμαστε έτοιμοι να πραγματοποιήσουμε μια επανεκκίνηση της συσκευής. Αν όλα πήγαν καλά, η συσκευή μας θα ξεκινήσει με το animation που κατασκευάσαμε! Με άλλα λόγια, θα ξεκινήσει με τον πιο εντυπωσιακό τρόπο που ξεκίνησε ποτέ κάποια συσκευή με Android :D

3. Ή τα αντίστοιχα αρχεία της Samsung, αν εργαζόμαστε σε συσκευή της συγκεκριμένης εταιρείας.



Πλήρη άρθρα που συμπληρώνουν το περιοδικό [**addenda**]. Το video podcast [**netcasting → deltaCast episodes**]. Άρθρα που μας ήρθε να γράψουμε, έτσι, απλά [**slash → /dev/random**]. Τα προκλητικά **mind hacks**. Τα βίντεο από τα προηγούμενα live streams [**netcasting → deltaStream**]. Ολόκληρα blasts from the past [**slash → var/backup/old**]. Τα πάντα ενδιαφέροντα **forums**. Το σημείο συνάντησης για τους φίλους του περιοδικού.

deltahacker.gr

Αληθινό, διασκεδαστικό hacking **για όλους**!

Skill: Advanced
Tags: Python, Py2Exe, Py2Exe2MSI, Py2App



by multiPetros

Βγάλτε βόλτα την Python [μέρος 2ο]

Στο προηγούμενο τεύχος εξετάσαμε συστήματα με τη βοήθεια των οποίων μπορούμε να πακετάρουμε βιβλιοθήκες ή και προγράμματα Python, προκειμένου να τα διανέμουμε εύκολα. Σ' αυτό το μέρος εστιάζουμε στα προγράμματα και κάνουμε ένα βήμα παραπέρα: Μαθαίνουμε πώς να παράγουμε αυτοτελή εκτελέσιμα αρχεία, ώστε τα προγράμματά μας να διακινούνται με ακόμα μεγαλύτερη ευκολία!

Στο πρώτο μέρος του άρθρου εξετάσαμε τη διαδικασία για την παραγωγή πακέτων EGG και WHEEL. Αυτά τα πακέτα προσθαφαιρούνται με άνεση σε μια εγκατάσταση της Python με τη βοήθεια των σχετικών εργαλείων (easy_install και pip) και, κάπως έτσι, οι βιβλιοθήκες και τα προγράμματά μας μπορούν να διανέμονται με ευκολία. Βέβαια, όταν μοιράζουμε ένα πρόγραμμα με αυτόν τον τρόπο, ο ενδιαφερόμενος πρέπει να εγκαταστήσει το σχετικό πακέτο και στη συνέχεια να εκτελέσει το κυρίως αρχείο (π.χ., main.py), τροφοδοτώντας το στον interpreter της Python.

Σε αυτό το άρθρο θα καταστήσουμε ακόμα ευκολότερη τη διανομή προγραμμάτων, δημιουργώντας εκτελέσιμα αρχεία για το περιβάλλον των Windows. Με αυτόν τον τρόπο, ο εκάστοτε χρήστης θα μπορεί να εκτελεί τα προγράμματά μας χωρίς τη μεσολάβηση της Python, όπως θα έκανε με οποιοδήποτε άλλο πρόγραμμα.

Προαπαιτούμενα

Για μία ακόμα φορά θα επιστρατεύσουμε τα εργαλεία distutils και θα τα συνδυάσουμε με τις λειτουργίες που παρέχει η βιβλιοθήκη py2exe. Ουσιαστικά, η εν λόγω βιβλιοθήκη αποτελεί μια επέκταση των distutils της Python. Για την εγκατάσταση της py2exe μπορούμε να στηριχτούμε στο αποθετήριο PyPI και να χρησιμοποιήσουμε το εργαλείο easy_install ή το pip. Εναλλακτικά, μπορούμε να κατεβάσουμε και να εκτελέσουμε το σχετικό πακέτο εγκατάστασης, από τη διεύθυνση `http://sourceforge.net/projects/py2exe`. Αφού προσθέσουμε τη βιβλιοθήκη py2exe, είμαστε έτοιμοι να ξεκινήσουμε τη μετατροπή των προγραμμάτων μας σε εκτελέσιμα τύπου EXE.

Για τις ανάγκες τις παρουσίασης επιλέξαμε να εργαστούμε μ' ένα πρόγραμμα που ενδέχεται να σας φανεί χρήσιμο και όχι με κάτι απλοϊκό και άχρηστο, του τύπου "hello world". Το πρόγραμμά μας αποτελεί ένα εργαλείο που προσθέτει αριθμούς γραμμών σε αρχεία απλού κειμένου και εκτελείται από τη γραμμή εντολών, όπως και τα περισσότερα εργαλεία στα συστήματα Unix. Φυσικά, στη συνέχεια του άρθρου δεν θα καταπιαστούμε με την ανάλυση του συγκεκριμένου προγράμματος, αλλά πιστεύουμε ότι, ακόμα κι αν θεωρείτε τη λειτουργία του εντελώς αδιάφορη, ο κώδικάς του μπορεί να κινήσει την περιέργειά σας και να λειτουργήσει διδακτικά.

```
#!/usr/bin/python
#
# lines.py - v1.0
# A line numbering program for text files
# Copyright (c) 2013, Petros Kyladitis
# This is free software distributed under the terms of GNU GPL 3
#

import argparse

def numbering(fin, fout, delimiter, lzeros=True, verbose=False):
    #if output file path not set, use input path and append "-line-
    numbered"
```

```
    if fout == "" :
        fout = fin + "-line-numbered"

    if verbose:
        print "Reading from: " + fin + " ..."

    #read lines from file an load them to a list
    fp = open(fin, "r")
    lines = fp.readlines()
    fp.close()

    if lzeros:
        #compute the digits of list size to fill with leading zeros
        digits = len(str(len(lines)))
    else:
        digits = 0

    #line counter
    i = 0

    #add the number (formatted with leading zeros and a space)
    for line in lines:
        lines[i] = str(i+1).zfill(digits) + delimiter + line
        i = i + 1

    if verbose:
        print str(len(lines)) + " lines processed"
        print "Writing to: " + fout + " ..."

    #write the list as line to the file
    fp = open(fout, "w")
    fp.writelines(lines)
    fp.close()

    if verbose:
        print "Done!"
```

```

def main():
    parser = argparse.ArgumentParser(description="lines v1.0 - A line numbering program for text files", epilog="(c) 2013, Petros Kyladitis. This is free software distributed under the terms of GNU GPL 3. For updates and more info see at <http://www.multipetros.gr/>")
    parser.add_argument("-v", "--verbose", action="store_true", dest="verbose", default=False, help="Verbose output")
    parser.add_argument("-l", "--no-leading-zeros", action="store_false", dest="lzeros", default=True, help="Don\'t add leading zeros")
    parser.add_argument("input", help="Input file path", metavar="INPUT_FILE")
    parser.add_argument("-o", "--output", default="", dest="output", help="Output file path (if not specified, the output filename is as the input, appended \'-line-numbered\' at the end)", metavar="OUTPUT_FILE")
    parser.add_argument("-d", "--delimeter", default=" ", dest="delimiter", help="Delimeter between line nubers and the begining character of each line (by default, used a space)", metavar="DELIMETER")
    args = parser.parse_args()
    try:
        numbering(args.input, args.output, args.delimiter, args.lzeros, args.verbose)
    except Exception as err:
        print(err)

if __name__ == "__main__":
    main()
```

Πριν προχωρήσουμε, σημειώστε ότι μπορείτε να κατεβάσετε τον κώδικα του προγράμματος από το https://bitbucket.org/multipetros/lines.py/get/8bf125ff4b01.zip.

Το αναπόφευκτο setup.py

Όπως αναφέραμε ήδη, η βιβλιοθήκη py2exe αποτελεί επέκταση των εργαλείων distutils. Επομένως, η εργασία μας θα περιστραφεί και πάλι γύρω από τα εν λόγω εργαλεία. Όπως πλέον γνωρίζουμε, κάτι τέτοιο γίνεται μέσα από ένα script το οποίο κατά παράδοση ονομάζεται setup.py και περιέχει μια κλήση προς την ομώνυμη συνάρτηση (setup). Ακολουθούν τα περιεχόμενα του αρχείου setup.py, που συγκροτήσαμε για τη μετατροπή του προγράμματός μας σε εκτελέσιμο των Windows:

```
01 from distutils.core import setup
02 import py2exe, sys, os
03
04 setup(
05     console=[{
06         "script":"lines.py",
07     }],
08     options = {
09         "py2exe": {
10             "optimize": 2,
11             "bundle_files": 1,
12             "compressed": 1,
13             "ascii": False,
14         }
15     },
16     zipfile = None,
17     #zipfile = "python.lib",
18     data_files=["README.md","LICENSE",],
19     version = "1.0",
20     name = "lines",
21     description = "A line numbering program for text files",
22     author = "Petros Kyladitis",
23     license = "GNU GPL 3 Licence",
24     url = "http://www.multipetros.gr",
25     )
```

Οι παράμετροι που ορίζονται από τη γραμμή 18 και μετά είναι γνώριμες από το πρώτο μέρος του άρθρου. Η πρώτη από αυτές προσδιορίζει τα αρχεία που συνοδεύουν το πρόγραμμά μας, ενώ οι ακόλουθες ορίζουν την έκδοση του προγράμματος, το όνομά του, την περιγραφή κ.λπ.

Τα άγνωστα στοιχεία εντοπίζονται στις γραμμές 5 έως 17. Αρχικά συναντάμε την παράμετρο **console**, η οποία συγκαταλέγεται στις προσθήκες του py2exe. Η συγκεκριμένη παράμετρος καθορίζει ότι το εκτελέσιμο που θέλουμε να δημιουργηθεί αποτελεί πρόγραμμα της γραμμής εντολών. Όπως βλέπετε, μέσα σε αυτή την παράμετρο ορίζουμε ένα ζεύγος κλειδιού–τιμής, με το οποίο δηλώνουμε το επιθυμητό όνομα για το εκτελέσιμο. Πριν προχωρήσουμε, αξίζει να σημειώσουμε μια ενδιαφέρουσα λεπτομέρεια. Αν το πρόγραμμά μας προοριζόταν για το περιβάλλον γραφικών, στη

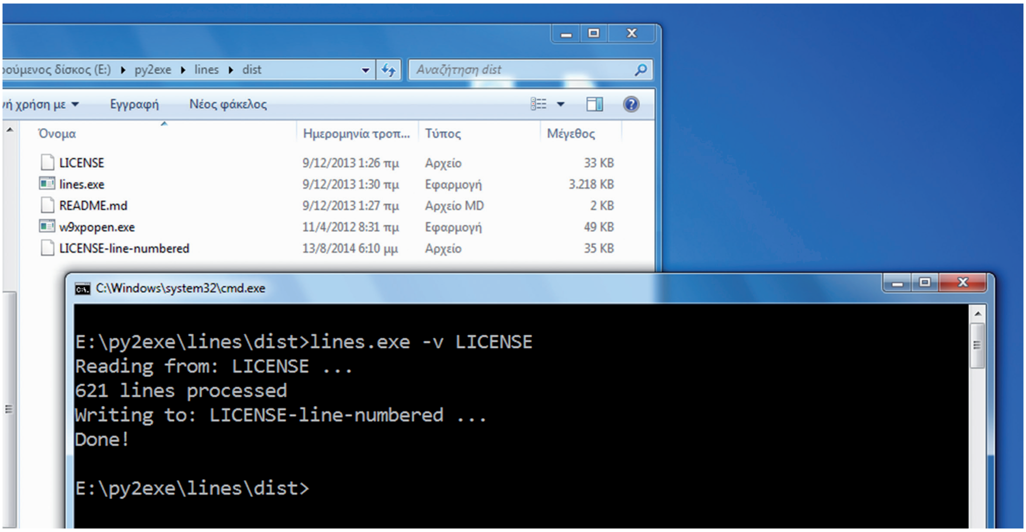
θέση της console θα έπρεπε να χρησιμοποιήσουμε την παράμετρο **windows**. Εναλλακτικά, αν το πρόγραμμά μας ήταν κάποιου είδους υπηρεσία και δεν περιελάμβανε interface για την άμεση επικοινωνία με το χρήστη, θα έπρεπε να χρησιμοποιήσουμε την παράμετρο **service**[1].

Ας επιστρέψουμε στο παράδειγμά μας, τώρα. Μετά την παράμετρο console ακολουθεί η **options**. Μέσα σε αυτήν ορίζουμε μια δομή δεδομένων που στην Python ονομάζεται dictionary[2]. Το όνομα αυτής της δομής είναι **py2exe** και, όπως υποψιάζεστε, περιλαμβάνει ρυθμίσεις για τη λειτουργία του πακέτου py2exe. Ας εξετάσουμε την ερμηνεία των ρυθμίσεων που πραγματοποιήσαμε εμείς:

- **Optimize.** Με αυτήν καθορίζουμε τις βελτιστοποιήσεις (optimizations) που θα πραγματοποιηθούν κατά την παραγωγή του εκτελέσιμου. Οι πιθανές τιμές που μπορούμε να δώσουμε εδώ είναι 0, 1 και 2 (0 για καμία βελτιστοποίηση, 1 για τις τυπικές βελτιστοποιήσεις και 2 για τις πιο προχωρημένες).
- **Bundle_files.** Αυτή η ρύθμιση καθορίζει το τι θα συνοδεύει το παραγόμενο εκτελέσιμο και δέχεται τις τιμές 1, 2 και 3. Με την τιμή 1 το εκτελέσιμο θα συνοδεύεται από όλες τις απαραίτητες βιβλιοθήκες, όπως επίσης και από τον interpreter της Python. Με την τιμή 2 το τελικό εκτελέσιμο θα συνοδεύεται μόνο από τις απαραίτητες βιβλιοθήκες κι όχι από τον interpreter, ενώ με την τιμή 3 το εκτελέσιμο δεν θα συνοδεύεται από κανένα άλλο κομμάτι κώδικα. Όπως αντιλαμβάνεστε, οι επιλογές 2 και 3 χρησιμοποιούνται όταν το εκτελέσιμο προορίζεται για χρήση σε συστήματα που περιλαμβάνουν ήδη την Python.
- **Compressed.** Αυτή η ρύθμιση καθορίζει τον τρόπο με τον οποίο πακετάρονται τα στοιχεία που καθορίζει η bundle_files. Όπως δηλώνει το όνομά της, η compressed καθορίζει αν τα πρόσθετα τμήματα κώδικα θα συμπιεστούν ή όχι. Αν δώσουμε την τιμή 1, οι βιβλιοθήκες και ο interpreter της Python θα τοποθετηθούν σε ένα πακέτο ZIP, ενώ αν δώσουμε την τιμή 0, θα τοποθετηθούν "χύμα" σε έναν ξεχωριστό κατάλογο.
- **ASCII.** Εξ ορισμού, τα εκτελέσιμα που δημιουργούνται από το py2exe περιλαμβάνουν τις βιβλιοθήκες χειρισμού των διαφόρων encodings. Αν το πρόγραμμά μας δεν κάνει χρήση αυτών των βιβλιοθηκών, μπορούμε να αποτρέψουμε την αυτόματη ενσωμάτωσή τους. Για αυτό το σκοπό προσφέρεται η παράμετρος ASCII. Δίνοντας την τιμή 0 αποτρέπουμε την ενσωμάτωση των βιβλιοθηκών που αναφέραμε και το τελικό εκτελέσιμο είναι αρκετά μικρότερο.

Στις γραμμές 16 και 17 φαίνονται δύο παραδείγματα χρήσης της παραμέτρου **zipfile**. Αυτή η παράμετρος συνδυάζεται με τη ρύθμιση compressed που είδαμε παραπάνω. Με την παράμετρο zipfile μπορούμε να καθορίσουμε το όνομα του πακέτου ZIP που θα περιλαμβάνει τις απαιτούμενες βιβλιοθήκες κι ενδεχομένως τον interpreter της Python. Αν δώσουμε την τιμή None (γραμμή 16), το συμπιεσμένο πακέτο θα ενσωματωθεί μέσα στο τελικό εκτελέσιμο. Εάν για κάποιο λόγο δεν θέλουμε να συμβεί κάτι τέτοιο, μπορούμε να δώσουμε στην παράμετρο zipfile μια οποιαδήποτε άλλη τιμή. Αυτό συμβαίνει στη γραμμή 17, που έχουμε δώσει την τιμή "python.lib". Όπως βλέπετε, όμως, η συγκεκριμένη γραμμή είναι απενεργοποιημένη με το χαρακτήρα έναρξης των σχολίων (#). Χρησιμοποιώντας την τιμή None, τα παραγόμενα εκτελέσιμα είναι πλήρως αυτοτελή και portable!

1. Θέλουμε να πιστεύουμε ότι αυτή η λεπτομέρεια θα σας δώσει μια καλή ιδέα για την παραπέρα βελτίωση του deltaLogger ;)
2. Η ίδια δομή δεδομένων υπάρχει και σε άλλες γλώσσες, αλλά με διαφορετικά ονόματα. Για παράδειγμα, στην PHP ονομάζεται "associative array".



Ο φάκελος dist περιλαμβάνει το εκτελέσιμο που προέκυψε από το script lines.py, καθώς και όσα άλλα αρχεία είχαμε καθορίσει με την παράμετρο data_files, εντός του setup.py. Όπως βλέπετε, ένα από τα πρώτα πράγματα που κάναμε ήταν μια γρήγορη δοκιμή του lines.exe, τροφοδοτώντας το με την άδεια χρήσης. Το πρόγραμμα λειτούργησε άψογα και σε ελάχιστο χρόνο είχε δημιουργηθεί ένα αντίγραφο της άδειας, στο οποίο είχαν προστεθεί αριθμοί γραμμών (LICENSE-line-numbered).

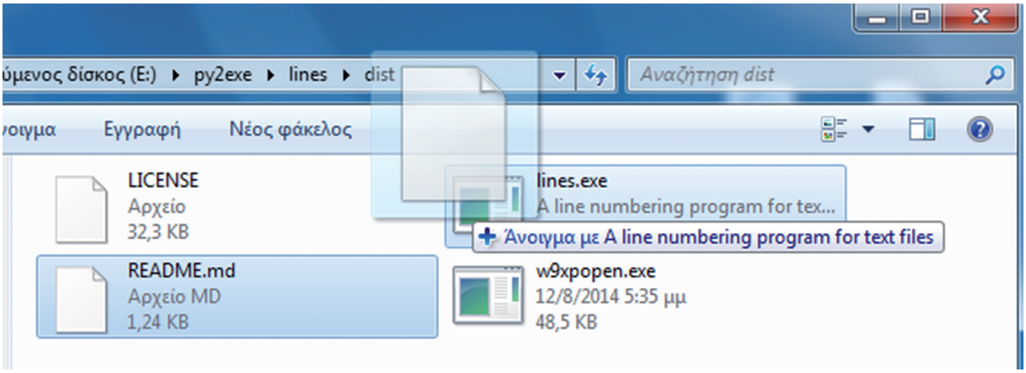
Τελικό βήμα

Έχοντας ετοιμάσει το απαραίτητο setup.py, απομένει ένα απλό βήμα για τη δημιουργία του εκτελέσιμου αρχείου. Ανοίγουμε ένα παράθυρο της γραμμής εντολών, μεταβαίνουμε στη θέση όπου βρίσκεται το setup.py κι εκτελούμε το εξής:

```
python setup.py py2exe
```

Η εκτέλεση του setup θα ολοκληρωθεί σε ελάχιστο χρόνο και, κατά τα γνωστά, θα παρατηρήσουμε ότι έχει δημιουργηθεί ένας φάκελος με το όνομα dist. Μέσα σ' αυτόν βρίσκεται το εκτελέσιμο που προέκυψε από το script, καθώς κι όσα αρχεία είχαμε δηλώσει ότι θέλουμε να συμπεριληφθούν. Με περίσσια περηφάνια, πλέον, μπορούμε να ξεκινήσουμε τη διανομή του προγράμματός μας, μοιράζοντας τα περιεχόμενα του φακέλου dist. Το πρόγραμμά μας είναι έτοιμο προς χρήση και δεν απαιτεί την παρουσία του interpreter της Python, ούτε και κάποιας βιβλιοθήκης!

Σε αυτό το σημείο αξίζει να διευκρινίσουμε μια λεπτομέρεια. Όπως είναι πιθανό να αντιληφθήκατε, με τη διαδικασία που παρουσιάσαμε δεν πραγματοποιήθηκε κάποιο είδος μεταγλώττισης. Το py2exe δημιούργησε ένα εκτελέσιμο πρόγραμμα, το οποίο ενσωματώνει τον πηγαίο κώδικα, τις απαιτούμενες βιβλιοθήκες και τον interpreter της Python. Όταν καλούμε το συγκεκριμένο εκτελέσιμο, ο πηγαίος κώδικας τροφοδοτείται αυτόματα στον interpreter και ξεκινά η εκτέλεσή του. Φυσικά, όλα αυτά πραγματοποιούνται με τρόπο που δεν γίνεται αντιληπτός από το χρήστη. Έτσι, ο κώδικας που έχουμε γράψει σε Python μοιάζει να εκτελείται σαν ένα φυσιολογικό εκτελέσιμο των Windows. Μάλιστα, το εκτελέσιμο που παράγεται με αυτόν τον τρόπο συνεργάζεται άψογα με το σύστημα. Για να καταλάβετε τι εννοούμε, σκεφτείτε το εξής: Το πρόγραμμα που μετατρέψαμε στην παρουσίασή μας λειτουργεί στη γραμμή εντολών κι απαιτεί να του δώσουμε σαν παράμετρο ένα αρχείο κειμένου. Το εκτελέσιμο που δημιουργήθηκε από το py2exe λειτουργεί με τον ίδιο ακριβώς τρόπο, αλλά



Το εκτελέσιμο που δημιουργήσαμε δεν λειτουργεί αποκλειστικά από τη γραμμή εντολών των Windows. Λειτουργεί άψογα και μέσα από τον file explorer του συστήματος, με τη βοήθεια του drag'n'drop. Όταν ρίχνουμε ένα αρχείο κειμένου πάνω στο πρόγραμμά μας, το σύστημα εκτελεί το πρόγραμμα και του δίνει σαν παράμετρο τη θέση και το όνομα του σχετικού αρχείου κειμένου.

και με έναν επιπρόσθετο. Μπορεί να χρησιμοποιήσουμε τη λειτουργία drag'n'drop του Windows explorer και να σύρουμε επάνω στο εκτελέσιμο ένα αρχείο απλού κειμένου. Κάνοντας κάτι τέτοιο, το πρόγραμμά μας θα εκτελεστεί και το σύστημα θα εισαγάγει αυτόματα σαν παράμετρο τη θέση και το όνομα του αρχείου κειμένου! Εν ολίγοις, τα εκτελέσιμα που παράγονται με το py2exe συμπεριφέρονται ακριβώς όπως θα περίμενε κανείς από ένα εκτελέσιμο των Windows :)

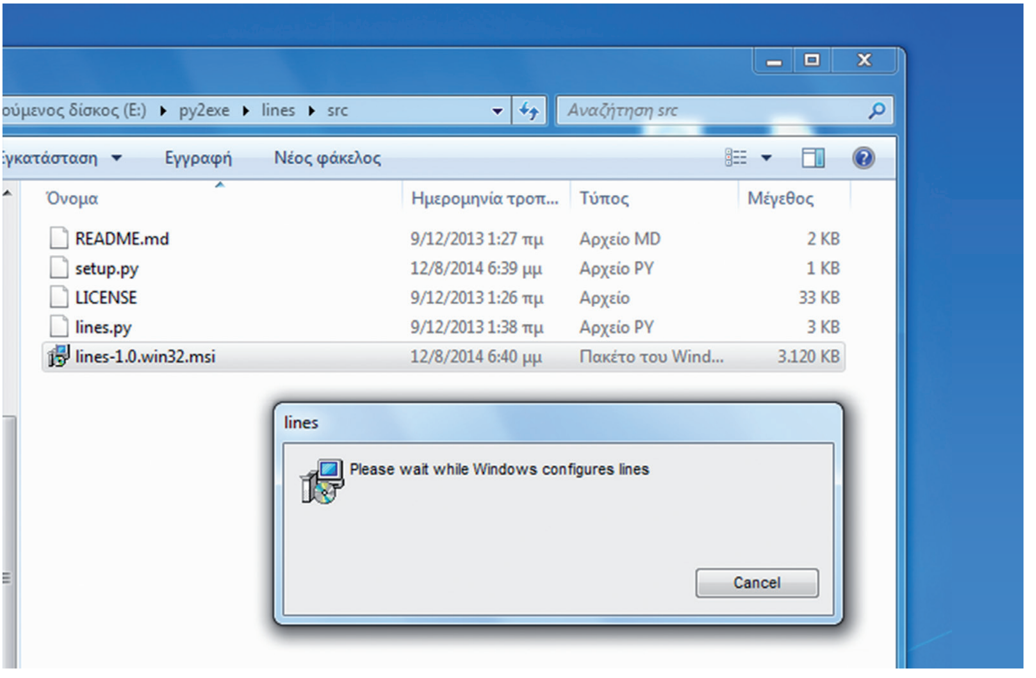
Απόπειρα βελτίωσης...

Η εργασία μας θα μπορούσε να ολοκληρωθεί με όσα είδαμε παραπάνω. Ωστόσο το μεράκι μας δεν εξαντλείται τόσο εύκολα. Έτσι, σκεφτήκαμε να δημιουργήσουμε κι εκτελέσιμο το οποίο θα περιλαμβάνει οδηγό εγκατάστασης! Για το σκοπό αυτό ξεκινήσαμε την αναζήτηση ενός κατάλληλου εργαλείου. Πολύ σύντομα πέσαμε πάνω στο πακέτο py2exe2msi και η έκφραση της ευχαρίστησης σχηματίστηκε στο πρόσωπό μας — ή τουλάχιστον έτσι νομίζουμε. Το συγκεκριμένο πακέτο αποτελεί επίσης extension των distutils και, όπως δηλώνει τ' όνομά του, αξιοποιεί το φορμά MSI για τη δημιουργία οδηγών εγκατάστασης. Δυστυχώς, αναζητώντας περισσότερες λεπτομέρειες για τη χρήση του py2exe2msi καταλήξαμε σε αδιέξοδο. Η σχετική σελίδα του project στο Google Code δεν παρείχε καμία βοήθεια, ενώ και το ίδιο το project έμοιαζε ανενεργό. Παρ' όλα αυτά, το πείσμα μάς ώθησε να συνεχίσουμε την αναζήτηση και κάπως έτσι ξεκινήσαμε τη μελέτη του πηγαίου κώδικα. Το py2exe2msi στηρίζεται στο py2exe και μετά το ξεψάχνισμα του κώδικά του διαπιστώσαμε ότι δέχεται και μία παράμετρο. Με βάση τα ευρήματά μας, ανοίξαμε το setup.py και πραγματοποιήσαμε τις κατάλληλες προσθήκες. Συγκεκριμένα, στην αρχή του script προσθέσαμε μια γραμμή για την ενσωμάτωση του py2exe2msi:

```
import py2exe2msi.command
```

Στη συνέχεια, μέσα στην παράμετρο options δηλώσαμε ένα ακόμα dictionary, αμέσως μετά από αυτό το py2exe. Το νέο dictionary είχε το όνομα py2exe2msi και περιείχε μόνο ένα ζεύγος κλειδιού–τιμής:

```
"py2exe2msi": {
    "pfiles_dir": "some_folder_name",
}
```



Το πακέτο εγκατάστασης MSI που δημιουργήθηκε με τη βοήθεια του py2exe2msi. Όσο απλοϊκές είναι οι πρόσθετες ρυθμίσεις που συμπεριλάβαμε στο setup.py, άλλο τόσο απλές είναι και οι λειτουργίες του οδηγού εγκατάστασης. Η μόνη λειτουργία που προσφέρεται στο χρήση είναι αυτή της ακύρωσης!

Όπως υποψιάζεστε, με αυτό το "κλειδί" δηλώνουμε τον κατάλογο εντός του Program Files, ο οποίος θα δημιουργηθεί για την εγκατάσταση του προγράμματός μας. Μετά από αυτές τις δύο προσθήκες στο setup.py μεταβήκαμε στη γραμμή εντολών κι εκτελέσαμε το εξής:

```
python setup.py py2exe2msi
```

Αρχικά εκτελέστηκε το py2exe και δημιουργήθηκε το εκτελέσιμο με τον κώδικά μας. Στη συνέχεια εκτελέστηκε το py2exe2msi, το οποίο δημιούργησε ένα πακέτο MSI στην ίδια θέση με το εκτελέσιμο (φάκελος dist). Φυσικά, το πρώτο πράγμα που κάναμε αμέσως μετά ήταν και πάλι η πραγματοποίηση μιας δοκιμής. Η εγκατάσταση του προγράμματός μας καθώς και των συνοδευτικών αρχείων (README.md και LICENSE) ολοκληρώθηκε με επιτυχία, ενώ το πρόγραμμα καταχωρήθηκε και στον σχετικό κατάλογο της "Προσθαφαίρεσης προγραμμάτων", στον Πίνακα Ελέγχου των Windows. Ωστόσο, ο οδηγός εγκατάστασης ήταν εξαιρετικά λιτός και δεν παρείχε καμία ευελιξία στο χρήστη. Η εγκατάσταση πραγματοποιήθηκε στον κατάλογο που είχαμε ορίσει εντός του setup.py και δεν υπήρχε τρόπος να τον αλλάξουμε. Το μόνο που μπορούσαμε να κάνουμε κατά την εκτέλεση του οδηγού εγκατάστασης ήταν να ακυρώσουμε την εγκατάσταση! Επιπρόσθετα, δεν δημιουργήθηκε καμία συντόμευση προς το πρόγραμμα, ούτε στο desktop, ούτε στο μενού "Έναρξη" του συστήματος. Τελικά, η ενασχόληση με το py2exe2msi μάς δημιούργησε ανάμεικτα συναισθήματα. Πρόκειται για μία καλή ιδέα, αλλά η υλοποίησή της χρειάζεται ακόμα αρκετή δουλειά για να γίνει πραγματικά χρήσιμη και λειτουργική.

Μήπως πρέπει να πάρουμε το ζήτημα στα χέρια μας;

COOKIES



ΑΥΤΑ ΕΙΝΑΙ, ΡΕ ΦΙΛΕ...
...ΣΚΕΤΗ ΜΑΓΕΙΑ!
ΚΟΙΤΑ RESOLUTION, ΚΟΙΤΑ TEXTURES, ΚΟΙΤΑ DYNAMIC SHADOWS!...
ΠάΝΟΣ
ΠΛΕΟΝ Η ΠΡΑΓΜΑΤΙΚΟΤΗΤΑ ΕΙΝΑΙ ΤΟΣΟ ΡΕΑΛΙΣΤΙΚΗ...
...ΠΟΥ ΝΟΜΙΖΕΙΣ ΠΩΣ ΕΙΝΑΙ ΓΡΑΦΙΚΑ!